NEWSLETTER

No. 99-2 **JAN 99**

Task Force Eagle

Information Operations

"IO in a Peace Enforcement Environment"

CENTER FOR ARMY LESSONS LEARNED (CALL)
U. S. ARMY TRAINING AND DOCTRINE COMMAND (TRADOC)
FORT LEAVENWORTH, KS 66027-1350

FOREWORD

The Army's doctrine for Information Operations (IO) is relatively new. The first doctrinal manual for IO, FM 100-6, was published in August 1996 and focuses primarily on IO as a part of combat operations. However, units participating in the peacekeeping and peace enforcement operations of the 1990s have had to apply IO in military operations other than war (MOOTW) environments. Presently, there is no doctrinal information focused on implementing IO in peace operations.

This newsletter seeks to provide information on the application of Army Information Operations in a peace operations environment and an analysis of current doctrine as it is being interpreted in the field. Doctrinal concepts are applied to the category of MOOTW in general and to peace operations in particular. Specific examples are given to amplify the doctrinal discussions.

This newsletter is built on current doctrinal sources for Army Information Operations and its component disciplines and on observations from Task Force Eagle Operations JOINT ENDEAVOR, JOINT GUARD, and JOINT FORGE in Bosnia-Herzegovina. It provides commanders and their staffs a comprehensive document that shows how IO may be used to support operations in a MOOTW environment and provides tactics, techniques, and procedures (TTPs) as a starting point for mission analysis and course-of-action development.

If your unit has identified lessons concerning IO, or IO TTPs that work, please share them with the rest of the Army by contacting CALL at DSN 552-2255/3035, FAX DSN 552-9564/9583, or commercial (913) 684-2255/3035. Our e-mail address is call@leav-emh1.army.mil, and our WWW web page is http://call.army.mil. Be sure to include your phone number and complete address when contacting us.

MICHAEL A. HIEMSTRA
COL, FA
Director, Center for Army Lessons Learned

Information Operations (IO)

TABLE OF CONTENTS

CENTER FOR ARMY LESSONS LEARNED

Director
COL Michael A. Hiemstra
Managing Editor
Dr. Lon R. Seglie
Author
MAJ Arthur N. Tulak
Contributing Authors
CPT Robert Murphy, CALL
MAJ James Hutton, CALL
LTC Thomas Adams, CAAT-E Team Chief
MAJ Paul R. Brooks, PSYOP SME
LTC (Ret) Craig Jones, LIWA, IO SME
CPT Robert A.B. Curris, AFSCOORD, 1st AD
MAJ (Ret) Marc J. Romanych, LIWA
Editor plus Layout and Design
Mary Sue Winneke

CALL has many products of interest to the Total Force. A partial listing may be found at the back of this publication. We invite you to visit our web site at:

http://call.army.mil

The intent of CALL publications is to share knowledge, support discussion and impart lessons and information in an expeditious manner. This CALL publication is not a doctrinal product. The tactics, techniques and procedures (TTP) observed and reported in this publication are written by soldiers for soldiers. If you have, or your unit has, identified other relevant TTP for the U.S. Army, contact the

Managing Editor, Dr. Lon R. Seglie, at Coml (913) 684-3035/2255 or DSN 552-3035/2255; FAX DSN 552-3035/2255; E-mail: <segliel@leav-emh1.army.mil>. Articles must be submitted in either Word Perfect or Word format. Graphs, slides and clipart must be submitted separately from the document in either ppt, pcx or wpg format.

The Secretary of the Army has determined that the publication of this periodical is necessary in the transaction of the public business as required by law of the Department. Use of funds for printing this publication has been approved by Commander, U. S. Army Training and Doctrine Command, 1985, IAW AR 25-30.

Unless otherwise stated, whenever the masculine or feminine gender is used, both are intended.

NOTE: **Any publications referenced in this newsletter (other than the CALL newsletters), such as ARs, FMs, TMs, must be obtained through your pinpoint distribution system.**

LOCAL REPRODUCTION OF THIS NEWSLETTER IS AUTHORIZED AND ENCOURAGED!

★★★ ACKNOWLEDGEMENTS ★★★

The Center for Army Lessons Learned (CALL) wishes to acknowledge these organizations that contributed to the development of this newsletter:

Office of the Deputy Chief of Staff for Operations and Plans, Information Operations Division, HQDA, DAMO-ODI, Room BG761, The Pentagon, Washington, DC, 20310.

Director, Space and Information Operations Division, Deputy Chief of Staff for Combat Developments, Headquarters, TRADOC, Fort Monroe, VA 23561-5000.

Land Information Warfare Activity (LIWA), 8825 Beulah Street, Fort Belvoir, VA 22060-5246.

TRADOC, Program Integration Office, TPIO-TP (LIWA-KS), 415 Sherman Avenue, Fort Leavenworth, KS 66027.

Center for Army Tactics, U.S. Army Command and General Staff College, Fort Leavenworth, KS 66027.

Combined Arms Doctrine Directorate, U.S. Army Command and General Staff College, Fort Leavenworth, KS 66027.

Department of Joint and Multinational Operations, U.S. Army Command and General Staff College, Fort Leavenworth, KS 66027.

Headquarters, Task Force Eagle, Eagle Base, Tuzla Bosnia, Operation JOINT FORGE, APO AE 09789.

Chapter One
Introduction

"In their simplest form, (Information Operations) are the activities that gain information and knowledge and improve friendly execution of operations while denying an adversary similar capabilities by whatever means possible."[1]

Army doctrine for Information Operations is still relatively new (the keystone manual, FM 100-6, was published in August 1996) and applies primarily to combat operations. Information Operations (IO) in a military-operations-other-than-war (MOOTW[2]) environment is a developing area of doctrinal thought as Tactics, Techniques, and Procedures (TTPs) are still emerging and evolving in the field in the contingency operations of the 1990s, such as Operations JOINT ENDEAVOR (OJE), JOINT GUARD (OJG), and JOINT FORGE (OJF) in Bosnia-Herzegovina. The current Army IO doctrine manual emphasizes repeatedly that IO takes place across the operational continuum; however, as the doctrine focuses primarily on combat operations, leaders faced with the challenge of employing IO in MOOTW find themselves having to interpret doctrine to apply it to a different set of tasks.[3] In NATO peace operations in Bosnia, U.S. forces in Task Force Eagle have had to use a "trial-and-error" approach to IO planning.[4]

This newsletter is built on descriptive analysis of observations collected during peace operations on the disciplines now encompassed by IO doctrine, and on secondary-source research of open sources. The bulk of the newsletter addresses IO as practiced in Task Force Eagle, first under IFOR in OJE and then under SFOR in OJG. Its thrust is to apply the combat-focused Army IO doctrine to MOOTW in general terms, and then to peace operations in specific terms. Whenever possible, examples of doctrinal principles in application are provided to amplify and clarify the authors' analyses.

IO are not new, rather the concept of IO is a new approach to the way we conduct military operations which focus on controlling and exploiting information to support operations and achieve the desired end state. IO synchronize several information-based military operations, such as OPSEC, military deception, electronic warfare, psychological operations, civil affairs, and public affairs, that were previously "stove-piped" and independent of one another. By bringing all of these information-based and information-focused operations under one doctrinal framework, the Army ensures that all information operations are synchronized and mutually reinforcing, achieving synergy and unity of effort. The Army introduced its doctrine for IO with the publication of **FM 100-6, *Information Operations,*** on 27 August 1996. This new doctrine applies an organizing architecture to the many activities that focused on using information and information systems in support of military operations and details their inter-relationship. The publication of this keystone manual followed years of evolutionary debate in the Army and Joint community on what, exactly, constituted ***Information Operations*** and ***Information Warfare.***

FM 100-6 (August 1996) defines Information Operations as "continuous military operations within the MIE (Military Information Environment) that enable, enhance and protect the friendly force's ability to collect, process and act on information to achieve an advantage across the full range of military operations. IO include interacting with the global information environment and exploiting or denying an adversary's information and decision capabilities."[5] This definition specifies the operating environment for IO, which is the MIE. The MIE is that military portion of the Global Information Environment which consists of "...information systems (INFOSYS) and organizations - friendly and adversary, military and non-military, that support, enable, or significantly influence a specific military operation."[6]

IO are comprised of the three inter-related components of ***Operations, Relevant Information and Intelligence (RII),* and *INFOSYS.*** The Army uses three operations to conduct IO: 1) command and control warfare (C^2W); 2) civil affairs (CA); and, 3) public affairs (PA). Grouping the five elements of C^2W together with CA, and PA as specific IO provides a framework to promote synergy and facilitates planning and execution. All military activities conducted as part of these operations are classified within the two disciplines of C^2-Attack and C^2-Protect. C^2-Attack is offensive C^2W which is intended to gain control of the adversary's C^2 function in terms of his information flow and his situational awareness. Effective C^2-Attack allows friendly forces to either destroy, degrade, neutralize, influence, or exploit the enemy or adversary's C^2 functions. Successful C^2-Protect operations ensure effective C^2 of friendly forces "by negating or turning to a friendly advantage the adversary's efforts to influence, degrade, or destroy friendly C^2 systems."[7]

Operations.

C^2W Historically, the Army planned and executed the various elements of C^2W independently of one another.[8] Successful C^2W operations support the Army objective of achieving information dominance in any operational environment. Current IO doctrine combines the five elements of C^2W into one integrated approach. Emerging doctrine de-emphasizes the term C^2W and elevates the five elements of C^2W as components along with CA and PA. Under current doctrine, the five elements of C^2W are:

- ➜ **Operations security (OPSEC);**
- ➜ **Military deception;**
- ➜ **Electronic Warfare (EW);**
- ➜ **Psychological Operations (PSYOP); and,**
- ➜ **Physical Destruction.**

PA Public Affairs operations provide information about on-going operations to the American soldier and the American public. PA operations enable the commander to effectively operate with the media and pull information from the media that is of value to the commander and his forces. PA facilitates media on the battlefield to tell the story of the operation to the public. PA keeps the command informed through command information program, which explains the purpose of the operation to soldiers and leaders and what their expected role is in support of it.

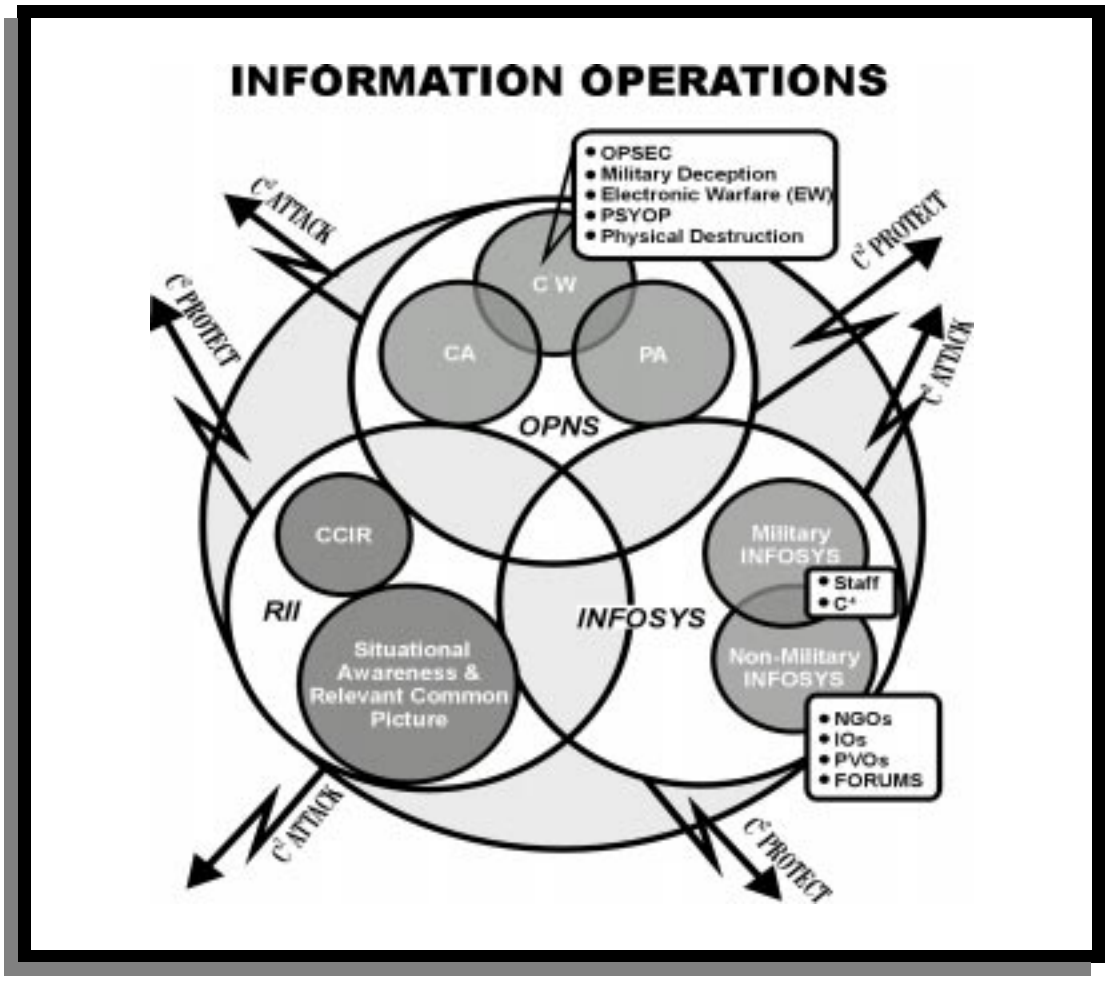
CA Civil Affairs operations secure local acceptance of U.S. forces by establishing the relationship between the military force, local civilian authorities, and interested international organizations (IOs), non-governmental organizations (NGOs), and private volunteer organizations (PVOs).[9] Successful CA operations support IO through their daily interface with key organizations and individuals operating in the MIE.

Relevant Information and Intelligence.

Relevant information is defined as - "Information drawn from the military information environment that significantly impacts, contributes to, or is related to the execution of the operational mission at hand...(RII) serves as the currency of IO."[10] Intelligence is "the critical sub-element of relevant information that focuses primarily upon foreign environments and the adversary. In support of friendly operations, intelligence helps produce a common, current, and relevant picture of the battlespace that reduces uncertainty and shortens the commander's decisionmaking process."[11] This situational awareness, built from RII shared throughout the force is referred to as the Relevant Common Picture (RCP). "Relevant information drawn from the MIE supports the creation of situational awareness that contributes directly to effective C^2 during all stages of the decision and execution cycle."[12] The commander specifies information requirements in the form of CCIR and PIR that drive the information collection process and assets.

INFOSYS.

"INFOSYS include personnel, machines, manual or automated procedures, and systems that allow collection, processing, dissemination, and display of information."[13] INFOSYS covers all of the links in the chain of actions and procedures that turn information into knowledge that will support the commander's decisionmaking process, maintain an accurate view of his battlespace, coordinate operations, and shape the MIE. INFOSYS disseminate the accurate view of the battlespace up and down the force giving leaders greater situational awareness (SA). INFOYS provides the means to share SA throughout the friendly force in the form of the Relevant Common Picture (RCP). "Relevant information drawn from the MIE supports the creation of situational awareness that contributes directly to effective C^2 during all stages of the decision and execution cycle."[14]✪



ENDNOTES, CHAPTER ONE

[1] Headquarters, Dept. of the Army, ***Information Operations,*** **Field Manual 100-6,** Washington, DC: USGPO, 27 August 1996, p. iv.
[2] The term MOOTW, which is acceptable Joint terminology, is used throughout this newsletter, as the Army's term of OOTW has been supplanted in some circles with Support and Stability Operations (SASO). For the definition of MOOTW, see ***The DoD Dictionary of Military and Associated Terms,*** **Joint Publication 1-02,** downloaded from http://www.dtic.mil/doctrine/jel/doddict/.
[3] Headquarters, Dept. of the Army, ***Information Operations,*** **Field Manual 100-6,** op. cit. The manual devotes only three pages to a discussion of the unique considerations for OOTW, a rather broad category of military operations, of which peace operations are merely a sub-set.
[4] Lt. Col. Stephen W. Shanahan, U.S. Army (Ret.), and Lt. Col. Gary J. Beavers, U.S. Army, **"Information Operations in Bosnia,"** ***Military Review,*** Vol. LXXVII, No. 6, November-December 1997, p. 61.
[5] Headquarters, Dept. of the Army, ***Information Operations,*** **Field Manual 100-6,** op. cit., p. 2-3.
[6] Ibid., p. 1-4.
[7] Ibid., p. 2-5.
[8] Ibid., p. 3-0.
[9] IOs are organizations with global or extra-regional influence – examples include the International Committee of the Red Cross, or the Organization for Security and Cooperation in Europe (OSCE). NGOs are transnational organizations of private citizens that maintain a consultative status with the Economic and Social Council of the UN. PVOs are typically non-profit organizations involved in humanitarian efforts. See Office of the Chairman of the Joint Chiefs of Staff, ***Joint Force Capabilities,*** **Joint Publication 3-33,** (Preliminary Coordination Draft): USGPO, 30 January 1998, p. IV-10.
[10] Headquarters, Dept. of the Army, ***Information Operations,*** **Field Manual 100-6,** op. cit.., 4-0.
[11] Ibid., p. 4-3.
[12] Ibid. p. 4-1.
[13] Ibid. p. 5-0.
[14] Ibid. p. 4-1.

Chapter Two
The Operations Environment

Role of IO in Peace Operations

In peace operations, the enemy is not one of the warring factions, but the conflict itself.[1] Diplomatic considerations predominate over purely military requirements and impose constraints on the force.[2] A common characteristic of peace operations has been the necessity to observe the principles of ***legitimacy*** and ***restraint.*** Although U.S. forces in a Peace Enforcement operation may have to apply lethal combat power during the initial stages, or as the result of acts which violate the terms of the imposed peace, the principles of restraint and legitimacy limit the efficacy of lethal combat power. The principle of ***restraint*** requires that forces **"apply appropriate military capability prudently,"** with due regard for collateral damage.[3] In peace operations, ***"When force must be used, its purpose is to protect life or compel, not to destroy...the conflict, not the belligerent parties, is the enemy...the use of force should be a last resort and, whenever possible, should be used when other means of persuasion are exhausted."***[4] Restraint is usually codified in Rules of Engagement (ROE) that restrict the use of conventional military force.

The focus of peace enforcement operations is to compel or persuade the former warring factions to abide by the terms of the ceasefire, peace agreement, or international sanctions or resolutions. IO may be one of the most critical and acceptable means of achieving stated objectives within the constraints of the ROE.[5] Army Peace Operations doctrine recognizes that the **"non-violent application of military capabilities, such as civil-military information and psychological operations (PSYOP), may be more important"** to achieving the desired end state.[6] Restraining the use of lethal combat power and conducting effective information operations can enhance both domestic and international perceptions of the legitimacy of the peace operation.[7]

The principle of ***Legitimacy*** must be overlaid onto all peace operations. Legitimacy is a condition initially derived by the peace settlement and the international legal mandate authorizing the peace operations force to enforce and keep the peace. Sustaining this legitimacy means sustaining the perception of the legality, morality, and correctness of all actions of the peace operations forces in the eyes of domestic and world public opinion and of the populace and civil-military leadership of the former warring factions (FWFs). Legitimacy requires impartiality in dealing with the FWF and other actors with interests in the conflict. In peace operations, the impartiality of the peace operation force is critical to success and the legitimacy of the operation. The peace operation force must demonstrate impartiality in all its dealings with the FWFs, showing no favor to either side. Key to sustaining perceptions of impartiality among the FWFs is the concept of ***transparency of operations.***[8] The concept of transparency of operations allows the FWFs to monitor the actions of the peace operation force as a confidence and security-building measure. In Peace Enforcement operations, transparency of operations must be balanced against the security and force protection needs of the friendly force.

Peace operations are carried out under the glare of public scrutiny via the media operating in the Global Information Environment (GIE). Employing the concept of transparency of operations serves to amplify this condition. The GIE consists of all organizations and systems outside the control of the military that process and disseminate information to national and international audiences. The news media comprise only a portion of the GIE, but one that can produce strategic-level implications from tactical-level events. Referred to as **"the CNN effect,"** the dramatic visual presentation of tactical events **"can rapidly influence public – and, therefore, political – opinion so that the political underpinnings of war and operations other than war may suddenly change with no prior indication to the commander in the field."**[9]

The strategic effects resulting from the broadcasting of tactical events via the GIE were clearly seen in adversary use of television images in the battle of Mogadishu in Somalia during UNISOM II, and the thwarted landing of the USS Harlan County LST in support of UNMIH in Haiti. In the former case, the televised image of Somalis dragging a dead U.S. soldier through the Mogadishu streets resulted in a strategic change of national policy and U.S. Forces withdrew precipitously.[10] In the latter case, the televised image of an orchestrated mob on the docks in Port au Prince, prevented the insertion of U.S. and Canadian forces by ship, leading to their complete withdrawal from the theater of operations.[11]

In peace operations, elements of the FWF and other adversaries opposed to the peace settlement will conduct IO targeted at U.S. Forces, U.S. public opinion, and world public opinion. Avoiding risk, adversaries will posture for the press, attempting to cause reactions through the resulting media reports, aimed at affecting strategic and operational-level decisionmaking of the peace operations force and the international community that supports it.[12] Adversaries will embellish reporting of actual events, or stage incidents for the media to broadcast to the other parties to the dispute, their allies, and nations contributing to the peace operations force to achieve strategic effects.[13] Public perception can put political pressure on nations to modify their participation in the peace operations effort – thus, adversary IO can strike at the strategic level and attempt to fracture the coalition of the multinational forces assembled for a peace operation.[14]

Other actors are present on the peace operations "battlefield" and may intrude into the MIE causing serious disruption of the operations of the peace-operations force. Elements of the FWFs operating in the MIE may consist of more than just their armed forces. These other actors include the local police forces, local and regional political and religious groups, terrorists, and even criminal syndicates.[15] Additionally, other organizations supporting the overall peace effort, but operating outside the MIE, may conduct independent IO which can affect the peace operations force. These other organizations include offices of the United Nations, International Organizations (IOs), Non-Governmental Organizations (NGOs), and Private Volunteer Organizations (PVOs). Effective liaison with the non-military supporting organizations can prevent contradictory or non-reinforcing information efforts and present a unified IO effort.

As the examples of adversary IO in Mogadishu, Somalia, and Port au Prince, Haiti, demonstrate, technological and military prowess are not requirements for effective IO, especially in MOOTW. Potential adversary IO in MOOTW will seek to integrate all elements of its power and capabilities to target friendly forces. The likely adversaries U.S. Forces may face in MOOTW will not be concerned about information superiority or dominance, and will seek only temporary advantages at critical points and times. The likely adversary in MOOTW will see western concepts of laws of conflict as an unnecessary handicap and will have few qualms or cultural aversions toward using deception, trickery, or civilian-run enterprise, or the media when implementing an IO campaign.[16] In MOOTW, friendly forces should expect that adversary IO will include all venues and media that can be manipulated by adversary leadership to include:

➜ Adversary PSYOP and psychological warfare (PSYWAR)[17] directed at the peace operation forces and propaganda for domestic consumption;

➜ Statecraft and public diplomacy used to generate media events that serve IO objectives;

➜ Censorship of domestic and international media, as well as misuse of all media to transmit propaganda and adversary PSYOP to all audiences.[18]

➜ Thuggery, coercion, brutal force and extortion to ensure the cooperation and passivity of the local populace with the agenda of the adversary leadership.[19]

Potential Adversaries in MOOTW include:

➜ Paramilitary or police forces overtly or covertly opposed to the presence or objectives of U.S. or friendly military forces;

➜ Organized military forces who are overtly or covertly opposed to the presence or objectives of U.S. or friendly military forces;

➜ Political, religious or social factions/groups, inside or outside the theater of operations (if these groups are overtly or covertly opposed to the presence or objectives of U.S. or friendly military forces on a specific military C^2 target set to oppose U.S./friendly objectives);

➜ **Individuals and organizations, inside or outside the theater of operations. If these actors are motivated to actively oppose the presence or objectives of U.S. or friendly military forces on a specific mission, they may try to deny, degrade, influence or exploit the friendly C^2 target set to oppose U.S./friendly objectives.**[20]

Bosnia

The Dayton Peace Accord (DPA) approved by the political leadership of the Federal Republic of Yugoslavia, the Republic of Croatia, and the Republic of Bosnia-Herzegovina (BiH) brought about a cessation of hostilities in the Bosnian civil war; directed the FWFs to withdraw behind a two-kilometer zone of separation (ZOS), and; authorized international peace enforcement operations in the republics of the former Yugoslavia.[21] In December 1995, acting under chapter VII of the United Nations Charter, the UN Security Council (UNSC) authorized member states to establish a multinational Implementation Force (IFOR) to implement the military provisions of the DPA.[22] The North Atlantic Treaty Organization (NATO) was designated as the controlling authority of the multi-national peace operation force, which included military forces from both NATO and non-NATO nations.

In Bosnia-Herzogivina, the Multi-National coalition that comprised the implementation and stabilization forces (IFOR and SFOR respectively) conducted ***peace enforcement*** operations to separate the FWFs and impose the military provisions of the DPA. Although IFOR successfully established a zone of separation (ZOS), and the military provisions of the DPA have largely been achieved, the ***peace enforcement*** component remained, and SFOR remained prepared to apply lethal combat power to compel compliance. Even with the transition to SFOR, the primary purpose of all operations in Bosnia remained the continued implementation of the DPA military provisions involving the Entity Armed Forces (EAF)[23] and maintenance of the peace necessary for the diplomatic, informational and economic instruments of power to operate. However, with the military provisions largely achieved, the emphasis on SFOR's military operations shifted to facilitating the accomplishment of the civil provisions of the DPA.

When Operation JOINT ENDEAVOR began in December 1995, the Army's IO doctrine was not yet codified in a single document; however, the components of IO were present, and IFOR conducted information operations daily. During the initial operations in Operation JOINT ENDEAVOR, the components of IO - C^2W, PA, and CA were all applied to attain information dominance. PA was used to compel compliance with the DPA when the TF Commander threatened to release to the international media information documenting non-compliance, obtained from ground and aviation reconnaissance of the Zone of Separation (ZOS), Civil Affairs and PSYOP teams, and the Joint Military Commissions.[24]

The first Information Operations Campaign for U.S. forces in Bosnia-Herzegovina to follow the new IO doctrine began in October 1996. Then MG Montgomery Meigs, the incoming commander of the 1st Infantry Division and the Multi-National Division-North (MND-N), coordinated with the U.S. Army's Land Information Warfare Activity (LIWA) at Fort Belvoir, VA, to assist in the development of an IO Campaign for the MND-N area of operations.[25] Another unique feature of the MND-N Information Campaign was that it supported a multi-national division.

To orchestrate the Division's IO, LIWA provided officers, civilians, and NCOs to form the Division IO Cell. Doctrinally, the ARFOR or land component commander is supported by a LIWA Field Support Team (FST) to form the IO Cell. **"When deployed, the LIWA FSTs become an integral part of the command's IO staff. To facilitate planning and execution of IO, LIWA provides IO/C^2W operational support to land component and separate Army commands and active and reserve components....LIWA acts as the operational focal point for land IO/C^2W by providing operational staff support to...land component commands...."**[26] The Multi-National Division-North (Task Force Eagle), commanded by the dual-hatted 1st Infantry Division Commander was a joint and combined force subordinate to SFOR.

The "battlefield" in Bosnia-Herzegovina has been one of a struggle of ideas competing for legitimacy and/or supremacy. On this battlefield, information is the weapon that is wielded through many forms to include propaganda, psychological operations, public affairs, and civil-military affairs.[27] Although IFOR and SFOR did not face off against an "adversary" in Operations JOINT ENDEAVOR, JOINT GUARD, and JOINT FORGE (OJE, OJG, and OJF respectively), the FWF leadership and populace were occasionally uncooperative and at times

bellicose toward IFOR/SFOR. During Operations JOINT GUARD AND JOINT FORGE, ***information operations*** were the primary means by which SFOR achieved effects in changing attitudes and reducing the barriers to implementing the civil aspects of the DPA. The SFOR Information Campaign Plan supporting this effort was built on eight pillars:

1. **Secure Environment**
2. **Demining**
3. **Economic Recovery**
4. **Displaced Persons, Refugees, Evacuees (DPRE)**
5. **Election results acceptance**
6. **The role of police in a democracy**
7. **Arms Control**
8. **Common Institutions supported by the DPA.**[28]

IO support battle command in peace operations by supporting the commander in imposing control over the battlespace and shaping it to achieve "situational dominance."[29] Through the non-lethal capabilities of IO, SFOR attacked the legitimacy of elements of the FWF leadership who attempted to block the further implementation of the DPA. SFOR IO targeted the adversary leadership's decisionmaking and C^2 and giving SFOR "the potential to control the adversary's decision-process tempo and even cause it to collapse."[30] Through a coordinated information campaign, SFOR could and did target the popular support base of adversary leadership and persuade the general populace to support the peace agreement and SFOR objectives.[31]

Task Force Eagle often found IO were the Division Main Effort as they comprised the most effective of the non-lethal fires the division could employ. In peace enforcement operations, the aim of IO is to support military operations that will establish "situational dominance" over the former warring factions and other actors. In Operations JOINT ENDEAVOR and JOINT GUARD in Bosnia, NATO and Coalition forces employed IO to know where the FWFs were and what they were doing at any given time.[32] The situational dominance IFOR and SFOR exercised over the FWFs was achieved by establishing and maintaining ***Information Dominance*** over the FWF civilian and military leaders and other potential adversaries. The division employed its Reconnaissance, Intelligence, Surveillance, Targeting and Acquisition (RISTA) assets, supplemented by non-traditional intelligence collectors and human intelligence (HUMINT), to maintain an information advantage over the FWFs sustained the division's situational dominance.[33]✪

Endnotes, Chapter Two

[1] "Every soldier must be aware that the goal is to produce conditions that are conducive to peace and not to the destruction of an enemy. The enemy is the conflict [itself]...." Headquarters, Dept. of the Army, ***Peace Operations,*** **Field Manual 100-23,** (Washington, DC: USGPO), 30 December 1994, p. 17.
[2] Headquarters, Dept. of the Army, ***Decisive Force: The Army in Theater Operations,*** **Field Manual 100-7,** (Washington, DC: USGPO), 31 May 1995, p. 8-14
[3] Headquarters, Dept. of the Army, ***Peace Operations,*** **Field Manual 100-23,** (Washington, DC: USGPO), 30 December 1994, p. 17.
[4] Ibid., pp. v and 17.
[5] Headquarters, Dept. of the Army, ***Information Operations,*** **Field Manual 100-6,** op. cit., p. 6-17.
[6] Headquarters, Dept. of the Army, ***Peace Operations,*** **Field Manual 100-23,** op. cit. p. v. Civil-Military Information is generally understood to be the provision of infromation to civil authorities on the military operations of the peace operations force. FM 100-23 introduces the term *civil-military information*, but does not provide a definition.
[7] Ibid., p. 18.
[8] Ibid, p. 16.
[9] Headquarters, Dept. of the Army, ***Operations,*** **Field Manual 100-5,** (Washington, DC: USGPO), 14 June 1993, p. 1-3.
[10] Frank J. Stech, **"Winning CNN Wars,"** ***Parameters,*** Autumn 1994, Vol. XXIV, No. 3, p. 38.
[11] Ibid.
[12] Headquarters, Training and Doctrine Command, ***Concept for Information Operations,*** **TRADOC Pamphlet 525-69,** Fort Monroe, Va: TRADOC, 1 August 1995, p. 5.
[13] Office of the Chairman of the Joint Chiefs of Staff, ***Joint Tactics, Techniques, and Procedures for Peacekeeping Operations,*** **Joint Publication 3-07.3,** (Washington, DC: USGPO), 29 April 1994, p. VII-8.
[14] Headquarters, Department of the Army, ***The Army in Multinational Operations,*** **Field Manual 100-8,** (Washington, DC: USGPO), 24 November 1997, p. 2-18.
[15] Headquarters, Dept. of the Army, ***Information Operations,*** op. cit., p. 1-3. Some examples from Bosnia: IO -- the Organization for Security and Cooperation in Europe (OSCE). PVO – Doctors without Borders, NGOs – the International Committee of the Red Cross, Political groups – the FWF political parties, Religious groups – the Association of the Women of Sebrinica. See also Headquarters, Dept. of the Army, ***Peace Operations,*** **FM 100-23,** op. cit., p. v, and pp. 83-85 for a partial list of IOs, NGOs, and PVOs relevant to peace operations.
[16] Erin Gallogly-Staver, Maj., U.S. Army, and Raymond S. Hilliard, Maj., U.S. Army, **"Information Warfare: Opposing Force (OPFOR) Doctrine -- An Integrated Approach,"** ***News From the Front!,*** Center for Army Lessons Learned, Fort Leavenworth, KS, September-October 1997, pp. 12-18.
[17] Psychological warfare (PSYWAR) – the planned use of propaganda and other psychological actions having the primary purpose of influencing the opinions, emotions, attitudes and behavior of hostile foreign groups in such a way as to support the achievement of national objectives. See **Joint Pub 1-02,** ***DOD Dictionary Military and Associated Terms,*** as amended 15 April 1998, pp. 349 and 350.
[18] Erin Gallogly-Staver, Maj., U.S. Army, and Maj. Raymond S. Hilliard, U.S. Army, op. cit., p. 14.
[19] Headquarters, Dept. of the Army, ***Battlefield Deception,*** **Field Manual 90-2, Washington, DC,** 3 October 1988, pp. 6-10. Although this manual is now obsolete, there is no follow-on Deception Manual yet published. Deception will be covered in the next edition of **Field Manual 100-6,** ***Information Operations.***
[20] Office of the Chairman of the Joint Chiefs of Staff, ***Joint Doctrine for Command and Control Warfare,*** **Joint Pub 3-13.1,** (Washington, DC, USGPO), 7 February 1996, p. V-7.
[21] The official name of the Dayton Peace Accord is the General Framework on the Agreement for Peace, or GFAP.
[22] **Field Manual 100-23,** ***Peace Operations,*** op. cit., p. 15, states that resolutions approved by a competent authorizing entity, such as the UN Security Council, express the political objective, international support, and define the desired endstate for peace operations.

[23] The Entity Armed Forces (EAF) are composed of the military forces and specialist police units of the two "entities" of Bosnia-Herzegovina -- the Bosnian-Croat Federation and the Bosnian Serb Republic (Republika Serpska). On the Bosnian-Croat Federation side, this includes the Croatian Home Defense Council forces (HVO) and the Bosnian Army. The term "Former Warring Faction" (FWF) refers to the three ethnic groups of Bosniacs (Moslems), Serbs, and Croats. When discussing peace operations in general terms, the term "FWF" will be used. When referring to NATO-led peace operations in Bosnia, the term "FWF" will be used when needed to highlight the three ethnic groups, "Entities" when referring to the two political systems, and "EAF" when referring to the military forces of those two political systems.

[24] Center for Army Lessons Learned, ***Initial Impressions Report - Operation JOINT ENDEAVOR – Task Force Eagle Initial Operations,*** (Unclassified, Distribution Limited, Fort Leavenworth, KS: CALL), May 1996, p. 58.

[25] Lt. Col. Gary Beavers, U.S. Army, and Lt. Col. Steve Shanahan, U.S. Army (Ret), **"LIWA Support to Operation JOINT ENDEAVOR/JOINT GUARD: Operationalizing IO in Bosnia-Herzegovina,"** ***Military Review,*** Vol. LXXVII, No. 6, November-December 1997, p. 53.

[26] Headquarters, Dept. of the Army, **Field Manual 100-6,** ***Information Operations***, op. cit. p. B-3.

[27] Lt. Col. Ronald T. Sconyers identified the "war of information" as comprising "the true battle area" in MOOTW in **"The Information War,"** ***Military Review,*** Vol. LXIX, No. 2, February 1989 pp. 44-52.

[28] Center for Army Lessons Learned, ***B/H CAAT 11 Initial Impressions Report,*** (Unclassified, Distribution Limited), Fort Leavenworth, KS: CALL, April 1998, p. A-18.

[29] Headquarters, Department of the Army, ***Intelligence and Electronic Warfare Operations,*** **Field Manual 34-1,** Washington, DC: USGPO, 27 September, 1994, p. 7-3.

[30] Maj. Gen. David L. Grange, U.S. Army, and Col. James A. Kelley, U.S. Army, **"Information Operations for the Ground Commander,"** ***Military Review,*** Vol. LXXVII, No. 2, March-April 1997, p. 9.

[31] Lt. Col., Dennis M. Murphy, U.S. Army, **"Information Operations on the Nontraditional Battlefield,"** ***Military Review,*** November-December 1996, Vol. LXXVI, No. 6, p. 16.

[32] Maj. Gen. David L. Grange, U.S. Army, and Lt. Col. James A. Kelley, U.S. Army, **"Information Dominance,"** ***Army,*** op. cit., p. 34.

[33] The term "RISTA" is used here deliberately, as opposed to the new term "Intelligence, Surveillance, and Reconnaissance," or "ISR," as the new term does not emphasize the Target Acquisition systems that support development of RII.

Chapter Three
Operations

In Army IO doctrine, the Operations component of IO consists of PSYOP, Physical Destruction, Electronic Warfare, Military Deception, OPSEC (the five elements of Command and Control Warfare), Civil Affairs, and Public Affairs. A peace operation information campaign will employ all these components to shape the battlespace. This chapter will examine how each of these components may be employed in peace operations. For each component, the following pages will first analyze how doctrine directs their employment in the broad category of MOOTW and then focus more narrowly on their employment in peace operations. Whenever possible, examples of doctrine in application are provided to amplify the analytical explanation.

All the components of IO are applied according to the disciplines of C^2-Attack and C^2-Protect. C^2-Attack in MOOTW is more than merely physical destruction or degrading adversary C^2 and includes all actions aimed at *influencing* and *co-opting* FWF C^2 systems.[1] Co-opting FWF C^2 in Bosnia meant using the Entity Armed Forces (EAF) systems to monitor their activities as they continued to use them to control their forces. The EAFs in Bosnia needed to have an effective C^2 systems to control their forces as they withdrew to comply with the military provisions of the Dayton Peace Accord.[2]

The five elements of C^2W support Army operations in both combat and MOOTW operations. Some of those involved in shaping IO doctrine have speculated that **"C^2W may replace air supremacy as the essential first step in operations."**[3] C^2W has a traditional warfighting orientation, both offensively and defensively, that focuses on ideas of threat, conflict, and the battlefield.[4] The emphasis of C^2W during MOOTW shifts away from the warfighting orientation to take in the broader and often political considerations associated with interacting with a variety of actors in the GIE.[5] The accepted Joint definition of C^2W specifies that C^2W is **"an application of Information Warfare in military operations."**[6] Information warfare covers the range of actions taken during conflict or crisis to achieve information superiority over an adversary. The *"warfare"* component of the term *information warfare* may seem to imply that IW applies only to combat operations. In fact, IW ***capabilities*** are employed in MOOTW to bring about the desired responses from several audiences to include the political and military leadership of the FWFs, the populace, and other actors.[7] The peace operations force employs its IW capabilities **"to preserve the peace, deter escalation of a conflict, and prepare the battlefield so that if a crisis escalated to conflict, the U.S. military can effectively employ (offensive IW) capabilities in a wartime scenario."**[8]

Joint C^2W doctrine specifies that the target of C^2-Attack is the information-dependent process and INFOSYS, whether human or automated. This demonstrates the relevance of IW concepts to MOOTW, where many of the FWF military, political, police, and social/cultural INFOSYS will not be automated, but will be forums of people and other media of communications that support decisionmaking.[9] Even in MOOTW **"C^2W offers the commander lethal and non-lethal means to achieve the assigned mission while deterring war and/or promoting peace."**[10] **"Adversary centers of gravity can be a function of the political, economic, military, sociological, ideological, or psychological context (or combinations thereof) which give rise to the presence of the [adversary]."**[11] Through offensive IO, the peace operations force can target such things as adversary leadership, decisionmaking and C^2, with the goal of controlling adversary decision process tempo, and attack the adversary's centers of gravity through non-lethal means to:

- ➜ **undermine the adversary's legitimacy or actions contrary to the provisions of a peace agreement;**
- ➜ **reinforce positive behavior in compliance with the peace accord;**
- ➜ **cajole compliance by stressing the responsibilities and actions required of the adversary under the provisions of the peace accord.**[12]

The Operations component of IO consists of C^2W, CA, and PA:

C^2W	CIVIL AFFAIRS	PUBLIC AFFAIRS
Psychological Operations (PSYOP)		
Physical Destruction		
Electronic Warfare (EW)		
Operations Security (OPSEC)		
Military Deception		

Psychological Operations (PSYOP)

PSYOP in Peace Operations achieve effects at the tactical through strategic levels. PSYOP support to the information campaign in peace operations seeks to enhance the legitimacy of the peace operations force and its mission, and to promote restraint on the part of the targeted audience. PSYOP support IO by developing products that develop understanding and favorable attitudes of the local populace toward the peace operation force; gain local support for the military effort; and, help attain the objectives of the friendly force.[13] By enhancing the peace operations force's legitimacy and promoting restraint, PSYOP improves security and force protection, while supporting accomplishment of the peace operation objectives.[14] PSYOP has been called the bridge to public diplomacy in MOOTW.[15] In that role, PSYOP can facilitate cooperation between the FWF and the peace operation forces and communicate the operational objectives to the target audience.[16]

PSYOP supporting the legitimacy of a peace operation must be based on the projection of truth and a credible message. To lend credence to the impartiality of the peace operation force and to maintain that credibility, the friendly force commander relies heavily on public information operations.[17] PSYOP comprise a large part of public IO as they transmit the peace operations force Information Campaign themes through print, radio, television, and loudspeaker media. PSYOP products and operations adhere to an IO strategy, expressed in the Information Campaign-approved themes ensuring consistency across all elements engaged in IO as information has no boundaries. PSYOP are considered C^2-Attack operations that often target the adversary center of gravity. PSYOP C^2-Attack operations in peace enforcement attack the legitimacy and credibility of the political systems of those opposed to the peace settlement, and publicize the beneficial reforms and programs being implemented as part of the peace settlement.[18]

In peace operations, several challenges face the peace operations commander in conducting effective information operations and civil-military information campaigns. The indigenous communications infrastructure is likely to be damaged or non-functioning. The FWFs may attempt to impose censorship over the remaining media to control the domestic populace. And finally, the local population may be illiterate and, therefore, difficult to reach through traditional print products.[19] PSYOP units can overcome communications disruptions with organic broadcasting and print production capabilities, and experience in preparing products tailored to their cultural and educational backgrounds.

In peace operations, political considerations drive military decisionmaking at the tactical through strategic-theater level of military operations.[20] During peacetime, the Department of State provides overall direction, coordination, and supervision of interdepartmental activities overseas, and may impose restrictions on the PSYOP messages and themes to be used.[21] Accordingly, PSYOP in multi-national and coalition peace operations may be referred to in innocuous terms. In Operation UPHOLD DEMOCRACY in Haiti, the PSYOP Task Force (POTF) established an in-country counterpart known as the Information Coordination Committee (ICC) to plan and coordinate IO throughout the operation. The ICC in Operation UPHOLD DEMOCRACY was chaired by the U.S. Embassy Public Affairs Officer (PAO) and included U.S. Agency for International Development (USAID), Department of Justice (DOJ) representatives along with officers from the JTF and Joint POTF (JPOTF).[22] In Bosnia, during Operation JOINT ENDEAVOR, PSYOP was referred to as "Military-Civil Relations" (MCR), and the PSYOP campaign was referred to as the "IFOR Information Campaign" and was controlled by the Coalition Joint Information Campaign Task Force (CJICTF).

PSYOP planning requires an inter-service and inter-agency approach.[23] Coordination with other U.S. Government (USG) agencies ensures that policies and plans supporting PSYOP objectives do not conflict with, and are mutually reinforcing with, messages from other USG agencies involved in the operation. Military PSYOP in peacetime or conflict may require coordination with several USG Agencies to include the Central Intelligence Agency, Board for International Broadcasting, the Departments of State, Commerce, Transportation, Energy, and Justice, the Drug Enforcement Administration, and the U.S. Coast Guard.[24] An important USG agency involved in conducting public diplomacy and determining foreign attitudes and perceptions is the U.S. Information Agency (USIA, formerly the U.S. Information Service (USIS)). During peace operations, the USIA is a part of the inter-agency team engaged in communicating with the people and governments of other countries. Military PSYOP can support these other USG agencies in public diplomacy initiatives and tasks.[25] In Peace-Enforcement operations, where the threat of force may be required to compel the FWFs to comply with the peace settlement, PSYOP, as a tool of the informational instrument of power, must be coordinated with the other national instruments of power – diplomatic, economic, and military.[26]

Although IFOR and SFOR conducted PSYOP activities according to the draft NATO doctrine for peace support psychological activities, the North Atlantic Council ((NAC) - the controlling political body of NATO) preferred the term "Information Campaign." This action addressed political concerns of the North Atlantic Council and coalition partners, some of whom were prohibited by national laws from using the term "psychological warfare" in connection with their military forces.[27] However, PSYOP, in support of information campaigns, are in accordance with PSYOP doctrine which specifies that PSYOP assets may support a commander's information and awareness program. In such cases, the commander must clearly distinguish that PSYOP assets are being used in a dissemination role only, not to project a PSYOP message. When appropriate, PSYOP assets can also disseminate command information products that explain the intent of military operations to target audiences.[28] In this role, PSYOP assets support CA civil-military information operations.

During the first two years of OJE and OJG, more than 1,000 PSYOP personnel deployed to Bosnia where they produced and distributed more than 12 million "products" including handbills, posters, a weekly newspaper, a monthly teen magazine, radio and television spots, and, for the children, comic books, soccer balls, coloring books, and even pens with the IFOR/SFOR logos.[29]

IFOR/SFOR PSYOP products supported several International Organizations (IOs) in implementing the civil aspects of the Dayton Peace Accord (DPA). The Coalition Joint Information Campaign Task Force (CJICTF) developed information programs supporting the SFOR IO campaign themes in support of various international organizations (IOs). One such PSYOP information program supported the United Nations High Commissioner on Refugees (UNHCR) focusing on the IO theme of *displaced persons and refugees* (a UNHCR responsibility). Another supported the Office of the High Representative (OHR), the diplomatic controlling agent of the NATO-led operation in Bosnia, focusing on the IO theme of *common institutions* (an OHR responsibility). A campaign focusing on the IO theme of *economic recovery* supported those civilian organizations with responsibility for that mission. And a campaign focused on the theme of successful elections supported the Organization for Security and Cooperation in Europe (OSCE) which was responsible for the execution of the Bosnian elections.[30] Coordination between military PSYOP units and civilian information agencies during peace operations is critical to ensuring that their information themes, messages, and products do not contradict each other. Adversaries can use such contradictions as ammunition to fuel hostile propaganda efforts.[31]

PSYOP's main role in C^2-Protect is to counter the adversary's hostile propaganda against the joint and combined force.[32] Discrediting hostile propaganda serves to maintain the legitimacy and freedom of operation of the peace operations force while having the corollary effect of driving a wedge between the adversary leadership and the populace, thereby reducing its base of support and undermining its confidence and effectiveness.[33] Those opposed to the internationally-imposed peace settlement will likely attempt propaganda intended to build resentment against the military force by portraying it as an occupying force with aims counter to the interests of their particular faction.

In support of C^2-Attack operations, Tactical PSYOP Teams (TPTs) collect RII and disseminate information to decisionmakers and the local populace. Operating in small teams, the TPTs are well-placed to provide information on the attitudes and intentions of the population. PSYOP personnel gain information of value to the intelligence

(G2 or S2) officer and the PSYOP effort through close contact with friendly and hostile persons. PSYOP personnel routinely report such information through intelligence channels.[34]

Psychological Operations (PSYOP) in Task Force Eagle (TFE)

PSYOP Radio Shows as Information Operations.

PSYOP teams in MND-N, operating out of base camps, successfully used local radio shows as a medium to conduct information operations during Operation JOINT GUARD (OJG) to reinforce Information Campaign themes and to provide the SFOR position on developing events. The Information Operations Field Support Team OIC, who oversees the actions of the IO Battle Staff, which includes PSYOP, is responsible for Information Campaign themes, of which PSYOP themes are a part.

During OJG, a "network" of 43 local radio stations within the MND-N Area of Operations disseminated information, in the form of SFOR and TFE press releases, and PSYOP messages. The network covered most of the AO and included stations that were marketed toward each of the three entities. Many of the stations in the affiliate network provided this service at no cost to TFE and were receptive to reading the PSYOP-scripted messages, playing the pre-recorded music tapes with Euro-pop, or using the press releases provided by the PSYOP Task Force (POTF). Some stations, mostly in the Republika Serpska, had to be induced into playing the tapes and scripts with payments of about 9 DM per minute.

The Brigade PSYOP Support Elements (BPSEs) assigned to support Battalion Task Forces in the Base Camps distributed to the indigenous radio stations pre-taped shows (known as "Mir-Mix tapes") consisting of popular European pop music, interspersed with messages supporting Information Campaign themes and explaining the SFOR mission and desired end state. Most radio stations in the AOR were willing to play the pre-recorded shows as the taped shows contained newer and more popular music than they themselves could obtain. Some stations required financial inducement to play the pre-recorded shows. During OJF, Mir-Mix tapes were also distributed to local cafes to be played out loud during business hours.

The PSYOP staff officer arranged radio interviews with local radio stations for Battalion Task Force Commanders, XOs, and other officials. These interviews were both live and recorded for airing at a later time. Before the interview would take place, the PSYOP staff officer would obtain the questions the interviewer would ask, and would suggest issues important to the success of the SFOR mission that the commander would like to talk about. The PSYOP element would prepare answers to the questions provided and get the JAG and PAO staff officers to review the questions and answers to ensure synchronization. The commander could then review the question/answer report and use it as a preparatory tool before the interview, or as a crutch during the interview. This technique, while effective, was intensely time-consuming to prepare and execute and should, therefore, be balanced with other aspects of the information campaign. The radio stations were paid for conducting the interview after the show aired to ensure that the interviewer would not stray too far from the original plan or attempt to pursue a emotionally charged or politically loaded line of questioning.

Another technique using local stations was to ensure that official press releases, which discussed events, policies, or programs which reinforced PSYOP themes, were translated and provided to the local stations for broadcast. These press releases served as scripts for the local broadcasters who relied heavily on external news sources. The local populace then heard a recognized local newscaster giving the SFOR press releases and thus supporting SFOR PSYOP themes. The advantage of this technique is that the radio-listening public is more likely to lend credence to the report when it is presented by a local radio personality. The PSYOP team monitored the radio broadcast, either on-site at the studio, by listening to the broadcast, or by tasking other elements to monitor the broadcast, to ensure that the intended message is getting out to the listening public.

Local radio shows are an effective medium for conducting information operations aimed at the local population. Both interviews of military leaders and pre-recorded programming can support Information Campaign and PSYOP themes in a convincing and effective manner.

Radio PSYOP Supports Information Operations Campaign.

During OJG, SFOR PSYOP expanded its reach into the arena of non-military information systems by building a commercial-style radio station, *Radio Mir*, to broadcast popular music and live shows with PSYOP themes interspersed within them.

The Military Information Environment (MIE) includes several Nonmilitary Information Systems including commercial and government-run news media.[35] In combat conditions, PSYOP has the capability to broadcast on adversary frequencies.[36] In Military Operations Other Than War (MOOTW), such as the Peace Enforcement operations in Bosnia, these products are subtler than the combat products designed to weaken the enemy's morale and induce him to surrender. Successful PSYOP in MOOTW **"are based on projection of truth and credible message…[that serve to discredit] adversary propaganda or misinformation against the operations of U.S./coalition forces [which] is critical to maintaining favorable public opinion."**[37] Although U.S. Forces did not face an "enemy" in Operations JOINT ENDEAVOR and JOINT GUARD, the FWFs did spread propaganda that was counter to SFOR's objectives and interests.[38]

During initial operations early in Operation JOINT ENDEAVOR, TPTs established the technique of using local host-nation stations to air live broadcasts of interviews with PSYOP soldiers.[39] Task Force Eagle PSYOP radio operations included using civilian commercial radio stations to air pre-recorded music programs that contained "commercials" in between popular music songs that reinforced PSYOP themes. One risk with this approach was, given these radio stations were outside military control, they could, potentially, broadcast propaganda masquerading as "news" that could counter the PSYOP messages.

To achieve more control over the medium, one of the Brigade PSYOP Support Elements (BPSE) established an FM radio station, Radio Mir, in the ZOS near Brcko at Camp McGovern to provide a radio platform under SFOR control that would provide the listening public on both sides of the ZOS a credible and unbiased source of information. Mir stands for Military Information Radio and is the Serbo-Croatian word for Peace. Radio Mir consisted of an FM transmitting tower and equipment belonging to the JPOTF (Joint PSYOP Task Force), supplemented with civilian sound equipment housed in a wooden building constructed by Brown and Root Services Company, and sound-proofed with locally-purchased materials. The 1st Infantry Division purchased civilian sound-mixing equipment and sound-proofing materials and coordinated with Brown and Root to construct the facility.

Before the new station was built, the BPSE had only been able to transmit pre-recorded shows on the transmitter and lacked any facility from which to broadcast live, or to record interviews or programs involving local leaders and civilians. The new facility allowed the BPSE to conduct live broadcasting to include call-in shows, and to coordinate, prepare, and subsequently transmit shows recorded in-house.[40]

Initially, Radio Mir only broadcasted pre-recorded shows sent from the JPOTF (known as the Coalition Joint Information Campaign Task Force or CJCICTF) in Sarajevo, but planned to air live interviews with SFOR and local civilian leaders, and call-in shows for young people to discuss peace. Initial operations were designed to build a listening audience by broadcasting primarily popular music. Having a radio station under direct military-control expanded the relationship built up between the BPSE and local radio journalists and broadcasters and added a new dimension to the BPSE's capability to produce shows that would appeal to all of the entities within the station's broadcasting radius.

Radio Mir's location on the ZOS made it accessible to journalists and broadcasters from all sides. Local broadcasters on hand for the grand opening were duly impressed with Radio Mir's technological capabilities and were already discussing ideas with the BPSE about what could be done in cooperation with the station. The BPSE Commander's concept for the station was to involve the local populations as much as possible and have them reinforce the PSYOP themes in their own words. Programming on Radio Mir included:

- ➜ **Current news five times a day.**
- ➜ **"Classic" rock and roll, "Top 40" hits, Rhythm and Blues, local area music, Eurohits.**
- ➜ **Interviews with SFOR commanders and the Office of the High Representative.**
- ➜ **Broadcast talk shows with guest radio station personalities from local stations.**

TTP: **U.S. and Coalition Forces can expand their reach into the non-military INFOSYS of commercial radio by creating their own commercial-style FM radio stations equipped with the latest in broadcasting and sound-mixing technology. This expanded access can strengthen PSYOP within the station's broadcasting radius and improve the public perception of the U.S. and Coalition Force and its objectives.**

BPSE Commander and Interpreter at Opening of Radio Mir

Airborne PSYOP in Bosnia - Commando Solo

EC-130E Commando Solo

A multi-purpose asset capable of conducting both PSYOP and EW, the EC-130E, *Commando Solo*, is an airborne platform "primarily designed for PSYOP."[41] Commando Solo can conduct psychological broadcast missions in the standard AM, FM, HF, TV and military communications bands. Missions in Bosnia were flown at maximum altitudes possible to ensure optimum propagation patterns. Highly specialized modifications had been made to the latest version of the EC-130E. These included enhanced navigation systems, self-protection equipment, and the capability of broadcasting color television on a multitude of worldwide standards throughout the TV VHF/UHF ranges.

Three Air National Guard EC130E Commando Solo aircraft were deployed from the 193rd Special Operations Wing in Harrisburg, PA, to a base in Italy, an hour flight across the Adriatic Sea from Sarajevo. This was a direct response to persistent hostile Bosnian-Serb radio and television propaganda from the Karadzic faction. This same wing flew missions into Haiti during Operation UPHOLD DEMOCRACY to broadcast messages under the call sign of *Radio Democracy* on one AM band and three FM bands.[42]

Operating from Brindisi, Italy, the Commando Solo EC-130Es were equipped with high-power transmitters for TV, AM, and FM radio broadcasting. The plane's EW capabilities also allowed it to operate as a jamming device. In this mode, Commando Solo had the potential to jam Bosnian-Serb hard-liners' television and radio broadcasts or simply overpower their signal and replace propaganda with PSYOP programs. When used to broadcast programming

over the adversary signal, the aircraft is performing a PSYOP function. The aircraft executed three test flights over Bosnia-Herzegovina in September, testing radio broadcasting equipment as a non-violent "show of force" by SFOR.

The show of force was in response to inflammatory anti-NATO and anti-SFOR propaganda broadcasted by Serbian Radio Television (SRT). SFOR had forcibly secured SRT transmitter towers in September 1997, returning them to SRT control after securing written assurances that the propaganda would stop, that more even-handed reporting would follow, and that international programming on the progress of the peace operation would be aired. The SFOR commander warned that failure to follow through on these promises would result in decisive action by SFOR.[43] Commando Solo gave SFOR the non-lethal means of quickly neutralizing SRT transmissions in the case of non-compliance. The Commando Solo successfully relayed broadcast programs from the SFOR radio station "MIR" (Peace) without disruptions.

In mid-October, unidentified elements inside the Bosnian Serb Republic (*Republika Serpska* or RS) sabotaged television transmitters, taking the legal government's programming off the air in much of the eastern part of the RS. The pro-Karadzic faction resorted to propaganda to claim that the lack of normal programming was due to the "illegal" actions of the Stabilization Force. Shortly afterwards, SFOR used Commando Solo in a live mission to transmit on a frequency normally used by Bosnian Serb TV, actively countering the adversary propaganda by explaining that the absence of normal programming was due to the actions of the Bosnian-Serb leadership.

Airborne PSYOP – Leaflet Operations.

The MC-130E Talon aircraft is equipped for leaflet-drop PSYOP missions.[44] Aerial leaflet operations in Bosnia, however, were conducted primarily by helicopter aviation. During the October 1997 operations centering on curbing Bosnian-Serb broadcast propaganda, TFE launched a parallel, supporting information campaign to the SFOR program to counter the Serb broadcasts. The division commander appeared on local television outlets, both in person and by videotape to counter the anti-NATO and anti-SFOR broadcasts. However, as much of eastern Bosnia was outside the range of these television stations, leaflet operations presented a means to ensure broader coverage. Air distributed leaflets were a medium of communication that could reach this audience. PSYOP personnel prepared the leaflets with organic assets.

The leaflets were written in a tone meant to educate, rather than inflame passions. These products stressed such themes as the role of officials in a democratic society, especially the role of police as enforcers of the law rather than political police. Other leaflets presented the facts concerning international aid and the enforcement of the GFAP.

These leaflets were distributed from helicopters over key cities and towns in the American-led peace enforcement zone in northeastern Bosnia and adjoining areas. This included every major Serb-held area in northern Bosnia where anti-NATO and the state-run media broadcast attacks on the GFAP. About 43,000 leaflets were distributed from the air and by soldiers on the ground. The leaflets presented information about democracy and responsible government, quoting democratic thinkers including such icons as Thomas Jefferson, John Locke, Plato and others.[45]

On 16 October 1997, TFE delivered by air, over the city of Brcko, leaflets which urged the inhabitants not to vote for Karadzic and his supporters, noting that the unequal distribution of funds from the international community (IC) was due to the recalcitrance of the Karadzic faction to back the DPA.[46] Later that month, U.S. helicopters dropped leaflets on the city of Bijeljina, in the RS, in preparation for the November municipal elections. These leaflets supported the Plavsic regime in Banja Luka.[47]

Leaflets represented a very small fraction of the printed PSYOP products used in Operations JOINT ENDEAVOR/GUARD as other, more effective print media were available to disseminate PSYOP messages. These other printed media included comic books, magazines, newspapers, and posters. Air-dropped leaflets in Bosnia achieved mixed results. Some citizens complained about their towns being "polluted" and having to clean up the litter after the air-drop operation, ridiculed the grammatical errors, and were insulted that such a technique was used.[48] The Bosnian population during Operations JOINT ENDEAVOR and JOINT GUARD was media-savvy and consumed information from established media sources with

"The Role of the Press in a Democracy."

predictable regularity. Accordingly, airborne leaflet drops were not deemed profitable, and leaflet operations were suspended after the conclusion of OJG.

PSYOP Print Operations[49]

The IFOR Coalition Joint Information Campaign Task Force (CJICTF), supporting the peace operation in Bosnia, arguably produced more diverse printed products than any other mission to date. They produced newspapers, newspaper articles, handbills, posters, magazines, comic-books, and flyers for both the military and civilian implementers of the Dayton Peace Agreement. The CJICTF employed both organic and local print production facilities and both organic and non-organic assets for disseminating them.

Early in the peace operation, the CJICTF prepared, produced, and distributed a newspaper called ***The Herald of Peace*****.** This weekly paper was developed as a means of informing the population of Bosnia about the roles of IFOR and the civilian agencies and some of the particularly sensitive articles in the General Framework Agreement for Peace (GFAP). The articles were written by members of the CJICTF Product Development Center (PDC), subject matter experts from IFOR, or were taken from open-source news articles. The paper, each edition of which numbered 150,000 copies, was initially published in Stuttgart, Germany, later in Zagreb, Croatia, and finally in Sarajevo, BiH. [50]

When they were published in Germany and Croatia, IFOR air assets transported them to Sarajevo, where they were distributed throughout the country. One of the non-organic assets used for distribution and dissemination was that the CJICTF made a contract with a local publisher to transport about 50,000 copies to kiosks, located throughout the Federation. Before the situation stabilized, members of the CJICTF "escorted" a local commercial printer's transport vehicles through the confrontation lines around Sarajevo to Kiseljak; from there, the trucks were able to travel safely to their destinations. The remaining 100,000 copies were disseminated by traditional methods where Tactical PSYOP Teams (TPT) conducted face-to-face distribution. The CJICTF published this newspaper for about 16 months, when it was replaced by a monthly magazine named the ***Herald of Progress*****.** Both of these periodicals proved to be popular and effective organs for information, primarily targeting the adult audiences in both entities, while serving the needs of the military and civilian administrators of the GFAP.

The Herald of Progress (HOP) was a dramatic departure from former, traditional PSYOP print journalistic endeavors. It was a "Madison Avenue-quality" monthly journal with pertinent articles, color photos, and political cartoons and commentaries. Additionally, the CJICTF decided to diminish the divisive nature of language by publishing articles in both Latinic and Cyrillic alphabet. [51] The HOP editor and the PDC Chief chose to experiment with combining articles in both alphabets in one edition. Use of this format more than doubled the number of articles that could be produced in a single edition.[52] Except for several negative comments from hard-line Croats, who refused to accept any publication in Cyrillic, this format received positive comments from all Bosnians: Moslem, Croat, and Serb alike. Many people who responded to a survey could not immediately recognize a different format, since they all read both Latinic and Cyrillic equally well. The market segment or target audience of the HOP was the adult audience.

The German OpInfo Battalion, assigned to the CJICTF, decided to "market" or target their magazine, ***Mirko,*** to teenagers. This periodical was one of the most popular and successful PSYOP products. The five-man German team in Sarajevo developed concepts and aligned each edition to support selected PSYOP campaign objectives. This method reinforced PSYOP messages to the whole Bosnian population. Mirko served as an excellent vehicle for opening a dialogue between TPTs and local adults through their children. Surveys indicated that adults enjoyed the magazine as well.

One of the most interesting and potentially far-sighted products was a "Superman" comic book, published by DC Comics. This comic book, conceptualized and supervised by CJICTF officers and linguists, showed Superman assisting several Bosnian children out of a minefield near their home. The product was lauded by the Mine Action Center (MAC) for being one of the most effective products they could use to educate children about the dangers of mines and unexploded ordnance (UXO). UN representatives indicated their interest in using the comic book in other MAC-sponsored mine awareness initiatives, hoping to translate the product for other countries rife with minefields, also.

The CJICTF also produced millions of copies of fliers, brochures, handbills, and posters, the majority of which served to inform the local population about some aspect of the GFAP or a specific situation, such as voter registration, elections, freedom of movement, and responsible activities in a democratic society. The Office of the High Representative (OHR), the Organization for Security and Cooperation in Europe (OSCE), and the International Police

Task Force (IPTF) testified that the CJICTF's print efforts were singularly and clearly responsible for successes in their areas.

The dissemination method that held the greatest potential for future positive PSYOP distribution was an initiative where the CJICTF had articles and advertisements printed in local newspapers and magazines. Many influential local news organizations agreed to print PSYOP products as a form of "public service announcement." The CJICTF paid for these advertisements, as would any other credible journalistic or advertising agency. This offered the potential for continued relationships when the military force inevitably draws down and a leaner PSYOP force remains in country.

The CJICTF deployed an organic Modular Print System (MPS) from home station as a primary print shop for most handouts and pamphlets. It was used to publish several editions of the ***Herald of Peace*** newspaper until contracts could be assured in Bosnia. Not counting the millions of copies of products produced for IFOR and SFOR, the MPS printed about 12 million copies of products for the civilian implementers of GFAP by mid 1997.

The print medium, when properly used and presented, offered the CJICTF a viable and important means of disseminating messages to the population of Bosnia. Print remains an essential medium, but it must be tailored to the audience. The media-sophisticated audience in Bosnia presented challenges that required updated technology and flexible thinking for the CJICTF.

Tactical PSYOP Team soldier posting printed product concerning the Brcko Arbitration.

Physical Destruction.

In combat operations, the commander accomplishes the mission through the application of lethal combat power in combined arms operations. He uses IO to disrupt or destroy enemy information systems, primarily through EW and physical destruction.[53] Physical destruction is the most effective means for denying the enemy use of his C^2 systems and achieving an information advantage in the application of force.[54] **In peace operations, the principle of restraint and the neutrality of the peace operations force mean that the lethal application of combat power is rarely the means to mission accomplishment.**

Of the five elements of C^2W listed in Chapter 1, ***physical destruction (PD)*** may seem outside acceptable constructs for use in a peace operation where lethal force is used only as a last resort. However, physical destruction is **"the application of combat power to destroy** or ***neutralize*** **enemy forces and installations."**[55] It is primarily in the *neutralization* of adversary C^2 functions and processes that physical destruction is manifested in peace operations. "One can 'target' a (C^2)] system without designating it for actual destruction," effective C^2W aims to defeat the adversary C^2 system, "whether by physical destruction or effective nullification."[56] The destruction of a target means that the adversary capability is degraded or shut down, either permanently, or for a specified period of time.[57] Three elements of combat power, namely maneuver, firepower and protection, are applied to achieve PD effects.

Although SFOR did not physically destroy any of the FWFs' ability to command and control their elements, IO were aimed at ***influencing*** their C^2 decisionmakers. In Operations JOINT ENDEAVOR and JOINT GUARD, C^2W also aimed at co-opting the FWFs' C^2 apparatus to facilitate their compliance with the Dayton Peace Accord and to monitor that compliance as well.[58] FWF C^2 facilities were targeted for ***destruction*** during early NATO air operations supporting UNPROFOR in autumn 1995, known as ***Operation DELIBERATE FORCE,*** during which there were 3,515 sorties against Bosnian Serb military positions. This NATO air campaign is credited for having pushed the Bosnian Serbs to the peace table at Dayton Ohio.[59] During the siege of Sarajevo, the combination of attacks by NATO aircraft delivering precision air strikes against Bosnian Serb Army (VRS) positions, and an attack with 13 Tomahawk land attack missiles against VRS C^2 facilities, disrupted VRS C^2 systems and achieved the termination of the bombardment of Sarajevo and convinced Serb troops to remove their heavy weapons.[60]

PD operations in peace operations focus on the ***neutralization*** of adversary capabilities. In determining whether or not PD operations apply, the IO planner must identify the adversary's means to affect the situation, and then target those means for neutralization. Tactics employed to neutralize the adversary's ability to affect the situation or exercise command and control include:

- **➜ Occupying or controlling access to facilities used by the adversary for C^3 and early warning;**
- **➜ Shutting down power sources for C^3 and early warning systems;**
- **➜ Delaying groups or individuals of the adversary's support base attempting to mass;**
- **➜ Arresting or detaining key individuals and instigators of the adversary support base to prevent them from fomenting disturbance at "hot spots."**

Physical occupation of, or controlling access to, adversary C^3 and early warning facilities is a means of temporarily denying the adversary use of those capabilities. If the peace operation force cannot occupy the facility or control access to it, cutting off its power may provide a less-intrusive means of temporarily depriving the adversary use of the facility's functions. Examples of C^3 and early warning facilities that could possibly be targeted for PD include: TV and radio transmitting towers and stations, police stations, air raid sirens, and radio frequencies used to transmit radio or telephone communications.

The adversary may attempt to counter physical destruction operations which use maneuver forces to physically occupy facilities by conducting demonstrations of massed angry crowds. If the adversary attempts this option, alternatives to the use of deadly force include control measures such as pre-planned or improvised roadblocks, cordons, and checkpoints; warnings; and demonstrations or shows of force.[61] Delaying the movement of adversary supporters through the use of checkpoints and road blocks denies the adversary the ability to mass. Typically, demonstrations carried out in Bosnia by the FWFs involved busing in crowds of supporters from outlying towns and villages to achieve mass. The demonstrators sought to dominate the situation by stretching the peace operations force and forcing them to spread their forces thinly as they attempted to monitor and control the situation. Road blocks need not be formal, and *ruses* may be used to send the inbound mobs on detour after detour.

Crowds need leaders and instigators to be set into action. Detaining key leaders and instigators before the crowd assembles removes the volatile agent from the combustible mix. If the crowd has already assembled, it may be possible to remove instigators and agitators attempting to ignite the crowd into action.

Physical Destruction Operations in TFE

Seizure of Bosnian-Serb Radio/Television Towers.

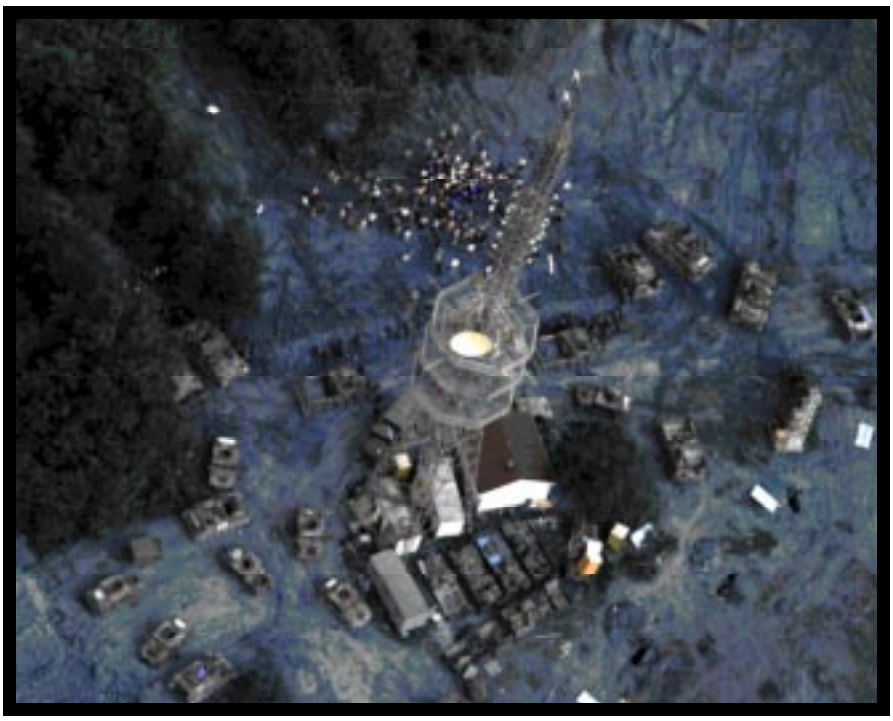
Following the civil war in Bosnia, much of the communications media lay in ruins. At the cessation of hostilities, newspapers and magazines were few, expensive, and had limited circulation. In such circumstances, broadcast media were extremely influential, despite the small number of operating transmitters. The broadcast media of the FWFs were politically driven and controlled. Reporting was biased by either omission of the truth, distortion through emphasis on only those elements of information which reinforced a political view, or outright disinformation, i.e., fiction-based propaganda. In May 1997, the North Atlantic Council granted authority to SFOR to take actions against any media undermining the peace accords.[62]

During the early summer of 1997, a power struggle erupted between the rival factions of the Bosnian Serb (Republika Serpska, or RS) leadership, that is, the RS President Bijlana Plavsic and the Bosnian-Serb member of the Bosnian presidency, Momcilo Krajisnik (loyal to the former RS President and indicted war criminal Radovan Karadzic). The struggle began when Madame-President Plavsic decided to dissolve the RS parliament and called for new elections in November 1997. The struggle caused a split within the RS state television, with journalists and editors from the Banja Luka studio deciding to split away from Pale direction after Pale manipulated a broadcast on SFOR searches in police stations. SFOR and OHR tried to exploit these developments to their advantage. SFOR and OHR encouraged SRT Pale to tone down its anti-Dayton, anti-NATO campaign and air programs on the DPA sponsored by the international community. In exchange for their cooperation, they would remain open, whereas non-compliance would bring military action.[63]

The pro-Karadzic, or Pale faction and its politically-controlled media continued the barrage of anti-SFOR propaganda and hate. SRT television stations for example, referred to the Muslim head of Bosnia's Presidency as "Alija Izetbegovic, Muslim murderer."[64] These same stations televised anti-SFOR propaganda to the Bosnian Serb audience attacking the legitimacy of SFOR and its mandate. One anti-SFOR propaganda item accused SFOR of using "low-intensity nuclear weapons," during the 1995 attacks on VRS positions around Sarajevo, Gorazde, and Majevica in 1995.[65] In another propaganda piece, Serbian Radio Television (SRT) showed alternating images of World War II German Army and present-day NATO forces while the commentator drew the comparison, likening SFOR soldiers to a Nazi occupation force.[66] NATO officials have expressed concerns that such "venomous propaganda" threatened the safety of the NATO-led peace operations force.[67]

Despite the efforts of both the High Representative and the OSCE, the dissident RS faction repeatedly refused to cease or moderate their broadcasts. After SRT Pale heavily edited a tape on the International Criminal Tribunal for the former Yugoslavia (ICTY) war crimes mission, using it to spread disinformation, the international community took direct action. Under the authority of the GFAP and orders from the NATO Council and the Office of the High Representative, SFOR seized four SRT transmission towers, considerably reducing the broadcast footprint of SRT. The seizure of these towers was a ***physical destruction mission*** in that SFOR targeted the TV transmitter towers for neutralization, which is a condition achieved by physical destruction operations. Within TFE, U.S. soldiers secured several transmitters used by media elements loyal to the pro-Karadzic faction. On October 1, 1997, TFE units executed the physical destruction operation, securing the Bosnian-Serb television/radio transmitter complexes on Hill 619 in Duga Njiva, Hill 562 near Ugljevik, Trebevica (near Sarajevo) and Leotar.[68] In pre-dawn raids, SFOR French, Polish, Scandinavian and American soldiers secured the sites and immediately fortified them against anticipated resistance.[69]

At Hill 619, U.S. Engineers operating Armored Combat Excavators (M-9 ACE) constructed protective berms for the troops, and cleared fields of fire, while other engineers emplaced a triple-standard concertina barrier around the site.[70] At Hill 562, 200 Bosnian-Serb protesters staged a 15-hour confrontation in which the protesters hurled rocks and attacked with clubs, damaging several vehicles.[71] **The application of combat power, in the form of maneuver to occupy ground, neutralized the adversary's ability to propagandize over the air waves.**



Seizure of SRT Tower at Hill 619.

Targeting Adversary Early Warning Devices for Destruction or Neutralization.

On 27 August 1997, SFOR received indications that Replubika Serpska (RS) police forces were attempting to take control of Police Stations in MND-N. This information followed a change in the status of Special Police units, some of which were equipped with armored cars, anti-tank rockets, anti-tank and anti-personnel mines, and other combat equipment. The change in status meant that these units were to be treated as military units and conform to the military provisions of the Dayton Peace Accord (DPA) under SFOR oversight, unless they were transformed into proper civil police units with a clear law-and-order mission. Special Police units in the RS declined to change their organization and, therefore, fell under the military provisions of the DPA, which meant that SFOR troops could inspect their facilities, and control their movements and training in accordance with Annex 1A.

In an operation intended to enforce compliance from the entity police forces, SFOR supported the International Police Task Force (IPTF) in an inspection of the Special Police units in Bijlijina, Brcko, and Jajna. As SFOR forces commenced operations early in the morning on 27 August, civil-defense sirens were used to mobilize the populace into action. Hostile crowds quickly massed in Brcko to demonstrate against the IPTF and the supporting SFOR forces.

The operation commenced during darkness at approximately 0200 to rapidly establish situational dominance while the populace was unaware. However, although the operation was initiated during the early morning hours, hostile crowds quickly gathered to thwart SFOR forces around the targeted facilities. At approximately 0500, two civil-defense sirens sounded in Brcko, alerting the populace to mobilize.[72] These sirens were complemented with radio broadcasts, one of which aired at 0700 urging the "Serb people" to respond to the **"call of danger and call to all citizens to assemble in the center of town...."**[73] One Sergeant on the scene reported **"They sounded an air defense siren and people just started bombarding us. We were getting pelted with bricks and blocks."**[74] During the remainder of the day, SFOR vehicles were damaged in attacks executed with "molotov cocktails," rocks, and bricks - soldiers were assaulted and injured. SFOR had lost the initiative to the hard-line Bosnian Serb faction leaders who orchestrated the demonstrators and who controlled the situation. RS Police refused to control the crowds and they achieved their objective of interfering with the IPTF Police site inspections. SFOR lost situational dominance early in this operation.

Rioters in Brcko confronting SFOR Soldiers, 28 August 1997. [75]

Following the operation, it became clear to the MND-N staff that in future operations, this warning and alert capability would have to be neutralized to allow SFOR to maintain the initiative and situational dominance. Neutralizing the civil-defense sirens to hamper the Bosnian Serbs' ability to muster is an example of a C^2-Attack Physical Destruction operation. C^2-Attack seeks to ***"gain control over our adversary's C² function...targeting personnel,* equipment, *communications, and facilities in an effort to disrupt or shape adversary C².*"**[76] Neutralizing adversary C^2 may be accomplished through electronic warfare, deception, and physical destruction. Neutralization is, therefore, a physical destruction effect, as the actual destruction of the facility or capability is not required. The definition of ***physical destruction*** in IO doctrine includes the ***neutralization*** of targets, which may be preserved and denied to the adversary selectively.[77] Although the sirens were very "low-tech" C^2, their effectiveness is irrefutable in light of the crowds that assembled in short order and numbered approximately 1,200.[78]

During peace operations in a MOUT[79] environment, in which the aim is to establish control over entities or functions of FWFs, the intelligence preparation of the battlefield (IPB) of adversary C^2 must address seemingly "low-tech" early warning capabilities such as civil-defense sirens. Denying the FWFs their warning and alert capabilities will delay and disrupt any organized response to friendly operations and ensure that friendly forces maintain the initiative and situational dominance.

Electronic Warfare (EW)

Electronic Warfare is the military use of electromagnetic and directed energy to control the electro-magnetic spectrum or to attack the enemy – it is divided into the three subdivisions of ***Electronic Attack, Electronic Protection,* and *Electronic Warfare Support.*** As stated before, C^2W in peace operations are primarily aimed at co-opting the INFOSYS of the FWFs to support the objectives of the peace operations force. In peace operations, electronic protection is continuous, as is electronic warfare support, while electronic attack is primarily a "be-prepared" or "stand-by" mission. Electronic Warfare Support (ES) measures can provide commanders the means to intercept, locate, and identify communications emitters used by FWF political and military leadership either for exploitation or for targeting.[80] In peace operations, EW assets are continuously collecting R.I.I. from adversary and FWFs' INFOSYS, exploiting those systems to maintain information dominance over the FWF political and military leadership.

The commander in peace operations plans EW for the contingency that friendly forces must act with force against the FWFs or other adversaries. The EW process is directed to be prepared to disrupt, degrade, neutralize, or decapitate adversary target acquisition, intelligence gathering, and C^3 systems while simultaneously protecting friendly C^3 systems from similar adversary actions.[81] Friendly EW capabilities are planned against targeted adversary C^3I systems to disrupt or destroy those systems when required. Successful implementation of EW operations demands that intelligence operations produce the required knowledge of the adversary INFOSYS and decisionmaking processes so that EW capabilities are accurately targeted for attack on adversary systems and positioned and postured for the defense and protection of friendly systems.[82]

Through EW, the commander may access the adversary's C3I systems to exploit intelligence through monitoring and manipulate those systems through deception to create a knowledge-based battlefield advantage that can be exploited by military forces to dominate the situation and the FWFs.[83] Intelligence acquired on FWF and adversary intentions through their INFOSYS provides a greater degree of force protection to the friendly force.[84] EW employed in this manner then provides a degree of transparency to the military, para-military, and police forces of the FWFs that permits monitoring of compliance with the established peace terms and provides early warning of potential violations or threats to the safety of the friendly force.

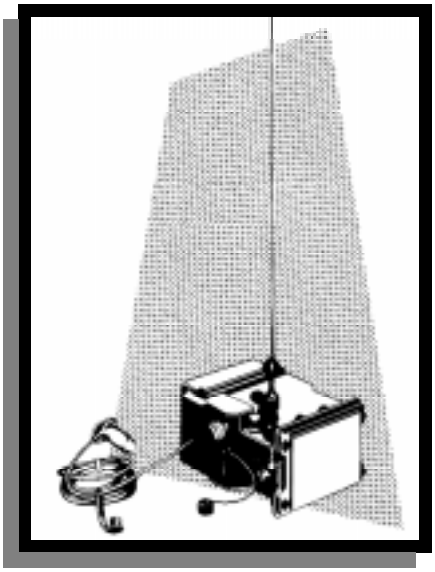
EW capabilities in TFE included jamming and sensor systems. In response to the virulent anti-NATO propaganda being disseminated over SRT television, SACEUR, on 28 August 1997, authorized use of jamming and other military action to stop the Bosnian Serb television propaganda campaign.[85] On 12 September 1997, three U.S. EC-130 aircraft deployed to Bosnia, to provide a jamming capability (see page 16, "Airborne PSYOP").

Tactical EW in Task Force Eagle initially focused on providing forewarning of EAF military activity and to assess their intentions and determine their resolve to use military force. As the military provisions were successfully implemented and the situation stabilized, the focus of EW operations was to monitor the EAFs for compliance, co-opting their C2 systems.[86] Much of the EW that took place in TFE consisted of using EW surveillance assets to monitor movement in the AO of the EAFs and noncombatants.

Ground surveillance technology, such as ground surveillance radar (GSR), and remote battlefield sensor systems, supported by night-vision devices, sensors, and thermal sights are useful in peace operations to observe and monitor situations. [87]

TFE ElectronicWarfare – Ground Surveillance Sensor Systems.

Ground Surveillance Systems (GSS) include ground surveillance radars (GSR) and remote sensors that track movement by acoustic, seismic, electromagnetic, or visual means.



Remotely Monitored Battlefield Sensor System (REMBASS)

While the doctrinal reference for the TTPs for REMBASS does not address the use of ground surveillance sensors in peace operations,[88] their use in past peace operations is a proven concept. The Multi-National Force and Observers mission in the Sinai uses remote sensors to monitor the demilitarized zone and compliance.[89] A demilitarized zone, or zone of separation (ZOS) is a common feature in peace operations. Task Force Eagle Teams used REMBASS and Improved-REMBASS (I-REMBASS) to monitor movement and activities in its AOR. The TFE GSS teams modified sensor employment and data analysis techniques to meet the needs of an environment which was non-linear and where there was no "enemy" per se.

The TFE MI battalion provided GSS teams to subordinate battalion task forces in direct support. The teams were composed of MOS 96R personnel who operated ground surveillance radars (GSR), REMBASS, and I-REMBASS. The initial emplacement of REMBASS "monitored the withdrawal of the military forces of the FWFs from the Zone of Separation (ZOS) and confirmed FWF reports of departure. As the factions withdrew, the systems were moved to monitor concentrations of FWF equipment, suspected areas of treaty violations, and force protection around base camps."[90] The teams provided support to perimeter security, a traditional mission, but were also employed in a variety of non-traditional roles and developed innovative tactics, techniques and procedures to support their new roles. TFE's REMBASS allowed remote monitoring of routes during key events, such as elections, resettlement operations, and provided alert, warning and indicators when large-scale movements were detected unexpectedly.

TFE developed new REMBASS employment techniques for peace operations, which included monitoring the movement of displaced persons and detecting movement along friendly, secured routes. GSS teams have conducted limited pattern analysis of data from sensors that have remained in place for extended periods. In a wartime environment, REMBASS are emplaced on the battlefield or in rear areas where movement is controlled. During OJG, GSS teams emplaced sensors in areas where the local populace had free or less restricted access. Mission requirements dictated the emplacement of sensors in areas settled or frequented by local civilians. The GSS teams regularly placed sensors in or near areas where friendly forces moved about in heavy equipment, and the civilian populace had free access. Although the teams found that sensors were more likely to become damaged, discovered or even stolen, the information the sensors provided proved to be more than worth the cost of the expendable sensors.

GSR

TFE employed Ground Surveillance Radars (GSR) to maintain situational awareness. GSS teams employed the AN/PPS-5C GSRs to monitor named areas of interest (NAI), cantonment areas, and intersections, and to provide force protection to the base camps. Radar teams positioned on top of high areas had excellent line of sight and early warning.[91]

GSS teams supported the command's requirement to monitor "unusual" or "suspicious" movement by the local populace and the resettlement of areas by refugees. For example, the teams emplaced sensors in named areas of interest (NAI) located in both rural and urban areas that had not been inhabited since the end of hostilities. Any movement in those areas, especially at night, would be considered unusual. Over time, the teams developed a database of sensor data about movement within those NAIs. They then conducted a limited pattern analysis of the data to assist TF S2 in determining its significance. By analyzing the data and tasking reconnaissance from other assets, the TF S2 and GSS teams were eventually able to determine what constituted unusual or suspicious movement, and to distinguish it from the planned resettlement of an area.

Operations Security (OPSEC)

> ***OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities; identifying those actions that can be observed by adversary intelligence systems; determining indicators adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and selecting and executing measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.***[92]
>
> **--Joint Pub 3-54**

OPSEC in peace operations poses unique challenges for the peace operations force as it engages in routine actions connected with maintaining the peace between the FWFs. Often we are unaware of the patterns we have established in our day-to-day, mission-to-mission operations, even in peace operations. Discernible patterns of operations give potential adversaries knowledge of our most likely course of action.

OPSEC may contribute to IO by slowing the adversary's decision cycle and providing opportunity for easier and quicker attainment of friendly objectives. OPSEC targets the adversary's ability to collect reliable, adequate, and timely intelligence, and, when integrated with other IO capabilities, shapes to the friendly force advantage the adversary's knowledge and beliefs about friendly operations. OPSEC denies the adversary critical information about friendly capabilities and intentions needed for effective and timely decisionmaking, leaving the adversary vulnerable to other offensive IO capabilities.[93]

Army OPSEC policy and operations doctrine state that the division OPSEC program is managed by the G3 who analyzes the commander's concept of operation to determine the essential elements of friendly information (EEFI) which must be protected from exploitation by enemy intelligence. The G3 develops appropriate OPSEC measures based on the G2's assessment of enemy intelligence collection capabilities and on the friendly indicators that may cause a compromise of the EEFI.[94] Achieving seamless OPSEC in peace operations also requires coordination with supporting agencies and departments from outside of the DoD.[95] OPSEC is a threat-oriented process consisting of five distinct actions: 1) Identification of critical information; 2) Analysis of threats; 3) Analysis of vulnerabilities; 4) Assessment of risk, and; 5) Application of appropriate OPSEC measures.[96] Although often described as occurring in five steps, the OPSEC process need not be applied in a sequential manner – "a recognized strength of the OPSEC process is that its elements are very fluid."[97]

OPSEC in peace operations is a careful balance between the transparency of operations required to demonstrate impartiality and force protection.[98] In a peacekeeping mission, transparency of operations will predominate, while in peace enforcement, force protection remains paramount.[99] Joint OPSEC doctrine requires coordination of the OPSEC plan with Public Affairs. In peace operations, this coordination is especially important because of the political sensitivity of these operations.[100] Army Peace Operations doctrine states that OPSEC in peace operations includes communications security (COMSEC); neutrality; prohibitions on photography; preparation of sites, accommodations and defensive positions; use of roadblocks and traffic control points; assessments of personnel vulnerabilities, personal awareness, security measures, sniper threats, coordination, and an evacuation plan.[101]

Given the combination of transparency of operations and a less constrained media presence in the peace operation battlespace, or "peace space," OPSEC is more difficult to achieve in peace operations. ***"The presence of the news media in the operational area, with the capability to transmit information on a real-time basis to a worldwide audience, has the potential to be a lucrative source of information to adversaries."***[102] Representing an even greater OPSEC challenge than the open media is the heavy presence of local civilian noncombatants interacting with the peace operations force on a daily basis. During NATO-led peace operations in Bosnia-Herzegovina, hundreds of civilians entered American base camps on a daily basis performing interpreter duties and other tasks. These persons may sympathize with, or have been members of, FWF military and para-military units, police or special police units, security forces, or intelligence forces of the former government.

Absent the immediate threat of combat in peacekeeping and mature peace enforcement, soldiers may become complacent regarding OPSEC.[103] ***Soldiers must be reminded that even unclassified information may be "sensitive" in nature, that is, its loss, misuse or unauthorized access by adversaries could adversely affect the national interest.*** Soldiers may divulge unclassified, but sensitive information with local national-hired workers, and local civilians as they engage in friendly conversations. Photography of sites occupied or used by the peace operations force should be prohibited. Photographs of base camps and other operational sites taken by soldiers of the peace operations force can easily end up in the hands of adversaries planning terrorism or espionage. Commanders must develop clear guidance on the prohibitions on photography for the friendly force to reduce OPSEC vulnerabilities.

The tradeoff between force protection and transparency is most evident in COMSEC as unsecure communications systems permit the FWF to monitor telephone conversations and radio traffic. Within TFE, the communications architecture and C^4I systems architecture is a mixture of U.S. and foreign systems characteristic of multi-national operations. However, several nonmilitary INFOSYS make up the overall architecture of communications for SFOR and Task Force Eagle. An example of the variety of systems cobbled together into a working whole is found in the telephones used by TFE. Two sets of commercially contracted telephone services, the two pre-existing UN phone systems, and the indigenous phone system all operated alongside U.S. and allied MSE-type phones. Such a complex array of systems presented greater C^2-Protect challenges as signals security (SIGSEC) and OPSEC measures had to be developed across all systems and links.

The computer INFOSYS employed by modern militaries provides substantial increases in information management during operations. TFE employed computers throughout the force, down to the company level for U.S. Forces. These computers were connected over secured and unsecured Local Area Networks and Wide Area Networks (LANs and WANs). Through these systems, U.S. Forces were able to share information in the form of FRAGOs, WARNOs, spot reports, briefings, etc., forming a Relevant Common Picture (RCP) that enhanced overall situational awareness (SA). The proliferation of computers represented a C^2-Protect information systems security problem: one IO analyst estimated that 50 percent of TFE's personal computers had suffered from computer viruses.[104] However, the computer INFOSYS also represented another C^2-Protect OPSEC challenge. Task Force Eagle employed teams from the Land Information Warfare Activity to identify vulnerabilities in its deployed automated information systems.[105] ***Elements opposed to the peace settlement could achieve tactical to strategic results by intruding into the peace operator's computer systems to alter data or introduce falsified data that would skew analysis and decisions made from that analysis that could jeopardize the mission.***[106]

FM 100-23, ***Peace Operations,*** lists Neutrality as an OPSEC principle in peace operations.[107] Neutrality reinforces the impartial relationship between the peace operations force and the FWF. Ensuring that all parties to the conflict receive the same information reinforces the perception of neutrality and enhances the legitimacy of the peace operations force. If any of the FWFs suspect that the peace operations force may be giving one side better information, the cooperation between the peace operations force and the FWFs could disappear. Even-handed neutrality removes any incentive for the FWFs to engage in espionage against the friendly force to obtain information they suspect is being withheld.

In peace operations, OPSEC, military deception, health and morale, safety, and avoidance of fratricide are all part of Force Protection.[108] OPSEC and military deception, are also elements of C^2W. Force protection measures that fortify these sites against terrorist attacks, infiltration, pilferage, surveillance, and sniper threats contribute to an improved OPSEC posture. Security measures, such as roving security patrols and sentries, Quick Reaction Forces (QRFs), and R&S patrols identify, correct, and prevent security deficiencies and threats, and maintain the soldier's personal awareness to the security threats around him. Acts of terrorism are a constant threat in most peace operations.[109] Elements not party to the dispute which prompted the peace operation, who are hostile to the United States, may see the deployment of U.S. Forces to a peace operation as an opportunity to strike against deployed American soldiers. All security measures should be coordinated with local police and military of the FWF and with civil agencies and charitable organizations operating in the AO.

Most peace operations have been multi-national operations. U.S. participation in peace operations brings U.S. information-based technology, weapons systems, intelligence-gathering, and other capabilities to the multi-national force. These capabilities are often shared, integrated, and synchronized in multinational operations, improving the capabilities of the entire force. This integration of U.S. and allied or coalition information, information-based process, and information systems creates additional vulnerabilities which an adversary can exploit by conducting information operations against the peace operations force.[110] In addition, the heavy intelligence aspect of peace operations, and the dissemination of classified information to lower levels of command mean that unit staffs can expect to handle more classified documents in peace operations. Many general-purpose force units are not accustomed to handling and safeguarding such volumes of classified information. These points only demonstrate that peace operations require even more attention to OPSEC, due to the heavy reliance on intelligence and the multi-national character of the peace operations force.

Multi-disciplinary counterintelligence (MDCI) analysis provides commanders with detailed assessments of hostile all-source intelligence and security threats near their operational bases and in their operational areas. These hostile threat assessments are critical to the unit's OPSEC and base defense programs. MDCI analysts compare their threat data base with the friendly force profiles provided by S3 OPSEC personnel to determine actual friendly vulnerabilities. The MDCI analysts evaluate the effectiveness of OPSEC measures.[111]

Within TFE, the Military Intelligence (MI) Task Force organized MDCI elements into Force Protection Teams (FPTs), allowing the MI Task Force commander to allocate his MDCI assets as the situation required. The FPTs were composed of CI Agents, interrogators, and civilian and military interpreters who worked in general support of TFE and in direct support of the subordinate battalion Task Forces including non-U.S. units. The FPTs conducted intelligence collection operations focused on force protection (CI-Force Protection Source Operations, or CFSO). Counter-intelligence doctrine states that CFSO "are focused on protection information on local terrorists, saboteurs, subversive activities, and other hostile activities affecting the security of deployed forces."[112] CI activities support OPSEC by providing information and conducting actions that protect friendly information and defend friendly INFOSYS against espionage, sabotage, or terrorist activities.[113]

In addition to the MDCI support, TFE requested an IO Vulnerability Assessment Team from the Land Information Warfare Activity to conduct a vulnerability assessment and recommend improvements to the Division OPSEC program.[114] Units may conduct their own assessments by conducting an OPSEC survey. OPSEC surveys are specifically designed to identify the patterns that potential adversaries may detect and provide that information to the commander.[115] No field manual is dedicated to explaining Army Operations Security (OPSEC) doctrine; however, **Army OPSEC policy is explained in AR 530-1, *Operations Security (OPSEC).***[116] OPSEC officers and commanders seeking to improve OPSEC programs in their units should contact the Interagency OPSEC Support Staff, 6411 Ivy Lane, Suite 400, Greenbelt, MD 20770-1405, or their web site at http://www.opsec.org/associations/IOSS.html, for OPSEC training publications, video tapes, and computer-assisted training programs. For soldier and small unit-level OPSEC TTPs employed by TFE, see **CALL Newsletter No. 97-1, *Tactics, Techniques, and Procedures from Operation JOINT ENDEAVOR,*** January 1997, pp. 46 and 47.

Military Deception

Throughout our military history, commanders have traditionally "viewed deception only as a warfighting need," but deception is applicable in peace operations.[117] **Army peace operations doctrine recognizes that the transparency of military operations required for traditional peacekeeping may preclude the use of deception, but note that deception operations may be both appropriate and necessary for peace enforcement.**[118] Deception is more difficult to achieve in peace operations where the operational-level objectives have more diplomatic content than military significance.[119] As with OPSEC, the characteristics of the modern information environment mean that deception operations require **"careful coordination with Public Affairs (PA) operations."**[120] **FM 100-7, *Decisive Force: the Army in Theater Operations,*** notes that most peace operations usually require little deception beyond normal OPSEC.[121]

Although conducting peace enforcement operations in Bosnia, SFOR policy during Operations JOINT ENDEAVOR AND JOINT GUARD disallowed the use of deception operations.[122] SFOR's requirement for the PSYOP and Public Information (PI) campaigns to be mutually reinforcing and complementary prevented the use of deception, which could compete with PI messages in the target audience.[123] While military deception is a legitimate function for peace enforcement operations, the multi-national and inter-agency character of these operations may complicate the deception plan as these elements could be easily confused by deception efforts if not aware of them in advance. Foreign Area Officers, MNF Liaison Officers, and SOF and State Department personnel should be used in the planning phase to ensure the messages sent to potential adversaries are perfectly clear.[124]

Tactical military deception consists of Distortion, Concealment, Manipulation and Falsification of indicators of friendly intentions, capabilities, or dispositions.[125] **In a peace operation, the FWFs may view it in their interest to practice deception aimed at either other FWFs or the peace operations force.**[126] Military deception is focused on desired behavior, not simply to mislead thinking. The purpose is to cause adversary leaders to form inaccurate impressions about friendly force capabilities or intentions, misappropriate their intelligence collection assets, or fail to employ combat or support units to their best advantage.[127]

Although SFOR policy did not permit deception operations, the METT-T analysis in future operations may lead to the use of deception to enhance force protection and OPSEC. The now obsolete, but not yet replaced, 1988 Battlefield Deception manual categorized deception activities into two types, which are useful here for understanding the basic fundamentals of deception operations: A (for ambiguity deception) and M (for misdirection deception). "A deception increases doubt in the target's mind and lowers the probability of a correct perception by taking from or adding to alternatives. M-deception reduces uncertainty in the target's mind by having him become convinced of a particular falsehood. Either form of deception can be accomplished, incidentally, by telling only the truth."[128] During the Gulf War, General H. Norman Schwarzkopf's tactics of emphasizing certain aspects of operations to the media to build a deception story based on true facts is a convincing example of this principle and was a M-deception effort. His emphasis on the amphibious landing rehearsals, for example, convinced the Iraqis that such an operation was likely and caused them to tie up large numbers of men and equipment defending coastal positions.

The Operation DESERT STORM amphibious assault deception provides an example of how a viable branch plan not used can be the foundation of a deception plan.[129] The deception plan is often developed from a viable course of action not chosen during the concept development phase. The deception plan is, therefore, a viable branch that may be pursued if the actual plan is compromised; therefore, at the operational level, the deception plan is as important as the real operation.[130] If deception is used, the deception plan is closely guarded, and this makes coordination difficult, but coordination is essential to ensuring success of the plan.[131] Finally, the deception plan must be developed to ensure a close fit with the collection capabilities of the target for the intended target to receive the deception story.

Public Affairs (PA)

"Peace operations are carried out under the full glare of public scrutiny....Because reports of peace operations are widely visible to national and international publics, PA is critical in peace operations. News media reports contribute to the legitimacy of an operation and the achievement of political, diplomatic, goals. PA must monitor public perceptions and develop and disseminate clear messages."[132]

The Public Affairs Officer (PAO) is the commander's advisor on media relations, the effects of the media on operations, and the PA implications of current and future operations and events. The PAO manages two information programs for the commander: the public information program and the internal information program, perhaps more familiarly known as the Command Information Program. The public information program is directed at external audiences, while the internal information program is for the force itself. In executing the public information campaign, the PAO **"communicates accurate, balanced and credible information to critical leaders and the public to influence their perceptions, understanding and decisions."**[133] To be consistently effective, the public information campaign must be perceived as credible and must provide a reliably steady flow of timely, accurate and balanced information.[134]

Commanders use their internal information programs to communicate directly to soldiers and leaders, to explain the mission and their part in it. **"Soldiers need and want information from both external and internal sources and are interested in the public perception of an operation."**[135] The internal information program (formerly the command information program) is more than a post newspaper or processing hometown news releases; it is a force enhancement tool that provides an outlet for the commander to ensure that the force receives clear guidance and instructions on what is expected from them. The internal information program also helps soldiers to combat the effects of enemy propaganda or misinformation.[136] In executing both the public and internal (command) information campaigns, PA conduct C^2-Protect operations in refuting and defeating adversary propaganda, and in providing accurate and timely information on the operation to positively influence domestic, international and local opinion.[137]

PA in peace operations is a means to counter adversary propaganda and to overcome censorship. In peace operations, where one or more of the FWFs may oppose the objectives of the peace operations force, adversaries will exercise censorship and public affairs programs aimed at the local populace, using the media and other neutral players, such as NGOs, as the media to transmit propaganda and disinformation.[138] In MOOTW, adversaries can also be expected to use an old Soviet technique to "plant" disinformation in the local or international media, or with NGOs or PVOs, and then pick up the story to support its propaganda effort after it has been reported, repeating it in the media it controls as a credible message obtained from a third party source.[139] Voids in information supplied to the media by the peace operations force may likely be filled with hostile propaganda or media speculation.[140] By closely monitoring the various media, PA remains ready to defeat enemy propaganda, by whatever media it is disseminated. The purpose of such disinformation propaganda may be directed at weakening the unity of effort of the coalition force, just as the Iraqis attempted a divisive PSYOP campaign aimed at weakening the multi-national coalition force.[141]

The PAO is the link between the media and the military force. On the battlefield, or in MOOTW, the PAO is the facilitator between the media and military operations. In addition to communicating information in the public and command information programs, the PAO leverages his connections to the media to monitor national and international media, identify and assess information relevant to the operation, and provide another information source to the commander.[142] As part of the public affairs media strategy, such conditions will require deliberation with the media to determine the ground rules for the conduct of media on the battlefield and rules for reporting and citing sources. Ensuring the adherence to these ground rules is essential to accomplishing the PA mission.[143] In TFE, the PAO controlled media operations on the ground, specifying the ground rules for reporters, and facilitating their deployment with units in the field to let soldiers tell the Army story.

Missions for the PAO in Peace Operations include:

(1) **Commander's advisor on media relations and effect of media on operations.**
(2) **Controlling media access to certain parts of military operations.**
(3) **Preparing information releases.**
(4) **Communicating directly with the local media through press conferences to provide the official position of the peace operation force.**
(5) **Countering adversary's propaganda.**[144]
(6) **Communicating command information to the deployed force in theater, to families at home station, and to the public.**
(7) **Providing focused PA coverage as directed.**
(8) **Coordinating with CA and PSYOP to ensure consistency of public information, command information, civil-military information, and PSYOP messages without any compromise to PA credibility.**
(9) **Making visual products and information available to the media to tell the Army story.**[145]
(10) **Scheduling and coordinating media events for the commander.**

The PAO must have the capability to monitor the national and international media and identify and assess information relevant to the operation. The media will cover the operation from several perspectives and, in so doing, provide open-source intelligence on the operation that can contribute to RII on the battlespace. In addition, the PAO remains abreast of how the operation is being reported to ensure that domestic public support for the operation is not jeopardized by inaccurate or incomplete reporting. The extremely political nature of peace operations and the open, independent nature of reporting support the principle of making information readily available within the constraints detailed by the source of authority.[146] Command Information publications released to the public can have positive effects on public opinion and support for the troops deployed.

Task Force Eagle PAO formed a Joint Information Bureau (JIB) to provide timely information to the media and to track their activities and compliance with Army and DoD PA "ground rules for the media." The JIB maintained a ***Daily Media On-Hand*** report that provided the PA staff with an up-to-date status report on media in the AO as well as contact information to allow immediate notification.[147] The JIB was later renamed the Coalition Press Information Center, which reflected the multinational character of TFE. TFE used the CPIC as a platform for IO directed at both the international and local audiences. The CPIC director in TFE was a key figure in developing and implementing effective IO in support of the peace enforcement operation. The crucial mission of the CPIC was to provide assistance and advice to the command group daily on the media aspects of planned and current operations.[148]

To support PA operations in TFE, several Reserve Component (RC) Military Public Affairs Detachments (MPADs) were alerted and deployed to Operations JOINT ENDEAVOR, JOINT GUARD AND JOINT FORGE. The importance in getting PA on the battlefield early can be seen in the fact that the selected callup for RC PA units occurred significantly earlier than for other major RC augmentation for the operation. RC MPADs from 21 states deployed in the first three rotations of RC units to OJE.[149]

Commanders can enhance IO by making PAOs aware of "newsworthy" events within the command.

Press Conferences as Tools in Information Operations.

"C^2-Protect includes countering an adversary's propaganda to prevent it from affecting friendly operations, options, public opinion, and the morale of friendly troops."[150] --FM 100-6, *Information Operations*

TFE used its weekly coalition press conference as an IO platform to refute disinformation and propaganda disseminated by hardliners of the FWFs opposed to the implementation of the General Framework on the Agreement for Peace (GFAP). Press conferences comprise a valuable tool to U.S. and Coalition forces in conducting information operations designed to counter adversary propaganda and disinformation campaigns. The press conference forum was the most efficient and effective way for friendly forces to get the word out over the indigenous media to decisionmakers and the local populace.

On June 21, 1997, U.S. soldiers disestablished an illegal checkpoint operated by RS police near the town of Brcko. The UN International Police Task Force Checkpoint policy required all checkpoints to be registered and approved with the IPTF. The policy stated that **"unauthorized checkpoints will be removed, with SFOR support, if necessary, (and) ID cards of the police officers involved will be confiscated."[151]** The U.S. SFOR soldiers attempted to confiscate ID Cards and weapons of the RS police officers operating the illegal checkpoint. When the police officers resisted, the U.S. patrol exercised appropriate force in subduing the officers and confiscating their ID Cards and weapons.

In a June 23, 1997, letter to the Commander, SFOR, the Interior Minister of Republika Serpska (RS) accused American SFOR soldiers of using excessive force in dismantling an illegal checkpoint. The letter stated that the American SFOR soldiers **"in a hostile mood...heavily armed and ready to misuse their weapons,"** had **"jumped on the policemen, tied, searched and beat them, and took away their belongings."[152]** Interior Minister, a hardliner in the RS government, deliberately misrepresented the facts and fabricated a false version of events to derail support of SFOR among the RS populace.

In a June 27 Coalition Press Conference, the Director of the MND-N Coalition Press and Information Center used the press conference as a platform from which to "shoot down" disinformation by issuing a statement to the press representatives from all three FWFs. The Director strongly refuted the lies presented as information and presented the truthful account to the gathered media.[153] The denouncement was also released on PSYOP radio programs.

Another example of the press conference being used to counter adversary propaganda and disinformation occurred on July 4, 1997. On July 3, 1997, the official RS radio station controlled by hardliners loyal to indicted war criminal, Radovan Karadzic, aired a report which claimed that SFOR soldiers had been ordered to arrest the former RS President and fellow indicted war criminal, General Ratko Mladic. The report further stated that the arrests would be carried out by July 15, 1997.[154] The report was picked up and disseminated by Reuters News Service.

CPIC Press Conference, July 4, 1997

On the following day, at a regularly scheduled press conference at Tuzla Base, the Director of the Coalition Press and Information Center issued a statement refuting the disinformation and again presenting the truth, explaining that no such order had been made and that SFOR's mandate had not changed in any way. In both cases, SFOR was able to speak to the media representatives of all three warring factions and present the truth. **"Discrediting adversary propaganda or misinformation against operations of US/coalition forces is critical to maintaining favorable public opinion."**[155] The press conference proved to be a flexible and routine conduit for C^2 Protection aimed at countering propaganda.

TTP: ***Press conferences comprise a valuable tool to US and Coalition forces in conducting information operations designed to counter adversary propaganda and disinformation campaigns. The press conference forum is the most efficient and effective way for friendly forces to get the word out over the indigenous media to decision makers and the local populace.***

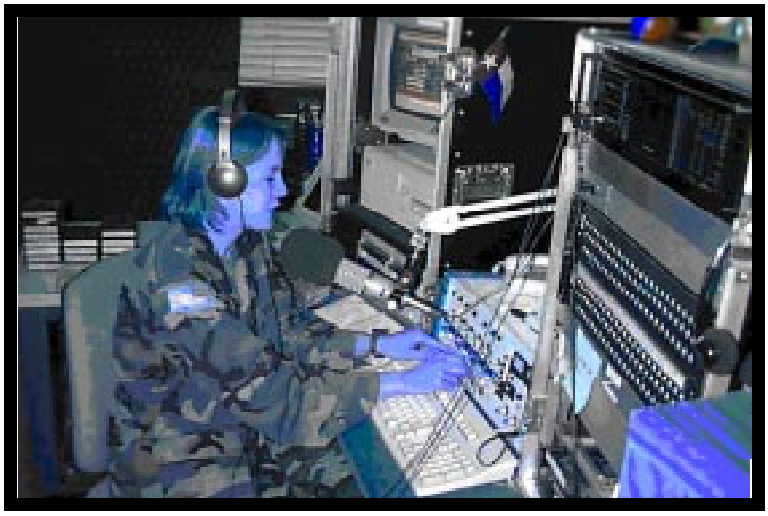
Internal Information Program.

The TFE Public Affairs Internal Information Program's primary product were the weekly Command Information Publications, ***The Talon,*** and the ***Tuzla Talk.*** Each ***Talon*** magazine had 12 pages produced on high-quality gloss paper with full-color photographs. The production schedule called for 5,500 copies of the magazine to be published every Friday. Additionally, the magazine was presented as a fully digitized product on a homepage dedicated to the operation - http://www.tfeagle.army.mil/ talon/index.html. The USAREUR Office of the Chief of Public Affairs (OCPA) emphasized in his initial planning guidance for OJE that it was important for soldiers to hear news from command information sources rather than speculation in the open press. [156]

Making the command information publication accessible over the Internet allowed families of deployed soldiers to keep up on current events in accordance with USAREUR's OCPA guidance to **"keep the soldiers and family members informed,"** and **"tell the troops and families first."**[157] A lesson from Operations DESERT SHIELD and DESERT STORM was that family support groups (FSGs) needed an information pipeline, which they did not have, for receiving command information from official sources.[158] Posting command information publications on the Internet provided that needed pipeline.

The ***Talon on-line*** also provided information to in-bound units and personnel, and provided on-the-ground information to U.S. Forces not in theater. It had a complete archive for retrieval. Articles for the magazine were developed and written by staff members from the magazine. The division PAO was the editor-in-chief and served as the publishing approval authority on behalf of the commanding general of the division. The second internal information publication the DIV PAO produced was the weekly ***Tuzla Talk*** newsletter. The ***Tuzla Talk*** newsletter was typically a two-page flyer which focused on events at Eagle Base, Guardian Base, and Comanche Base.

Another means of transmitting internal information to the soldiers was via Radio and Television operations run by the Armed Forces Radio and Television Service AFRTS, and Europe-based TV AFN. Broadcast assets from AFN-Europe were used to provide information and entertainment to U.S. and other soldiers and civilians deployed to the theater. The affiliate broadcast to listeners at all locations in Bosnia, Tazar, Hungary, and Zagreb, Croatia. On the same installation as Task Force Eagle headquarters, the radio station was established to provide information and entertainment on a 24-hour basis to U.S. and other soldiers. Although these elements had a mission other than command information, and were not under TFE PAO control, AFRTS radio and AFN both aired "commercials" that were often command information messages. Message breaks were filled with local interest items such as maintenance, safety, and command interest issues.



AFN Broadcaster in Action

One of the important contributions of the PA's internal information program was to provide the daily commander's media guidance. During initial operations in Operation JOINT ENDEAVOR, media representatives in TFE's area of operations often requested interviews with, or comments from, Task Force Commanders and their spokespersons on recent or rumored/known upcoming operations. To ensure that all levels of command spoke with one voice, the JIB, and its successor, the CPIC, maintained a daily report for the commander which contained "talking points" that included details on force flow, casualties, accidents, missions, FWF compliance, etc.[159] Information from the daily report was compiled on a weekly basis in the ***Information Operations Weekly Message for Commanders.*** The messages provided guidance to subordinate commanders via e-mail down to the company-level commander to prepare him for interactions with the media.[160]

The PAO also prepared individuals for interviews, when those interviews were approved by the JIB/CPIC. In one case during OJE, a Florida radio station director contacted the JIB to arrange an on-air interview with the Tuzla Armed Forces Network (AFN) morning radio disc jockey. The JIB passed the request to the AFN DJ ("dee-jay," short for disc jockey) who then contacted the Florida radio station. When the AFN DJ established telephone contact for the on-air interview, the Florida radio personality appeared to be friendly, but when the on-air interview began, the Florida DJ tried to bait and trap the AFN DJ into embarassing the Army by insulting both the AFN DJ and the Army. The JIB had prepared the AFN DJ with the weekly command messages and was able to stick to those messages and then terminate the interview when it became obvious that the Florida DJ had launched an "ambush interview" intended to discredit the DJ and embarrass the Army. This experience reinforced the importance of preparation and coordination tasks between the interviewer and interviewee, which include:

➜ Establishing what will be discussed during the interview to provide the lane boundaries for the interviewee.

➜ Developing a list of pre-interview questions to know what the interviewer is looking for.

➜ Establishing a set of ground rules that include being able to terminate the interview at one's discretion.[161]

Civil Affairs (CA)

Civil Affairs accomplishes three key tasks in peace operations:

1. Liaison between the military force and local civil authorities and engaged IOs, NGOs, and PVOs in the area of operations.
2. Builds and maintains local and regional public support for the military force and its objectives.
3. Provides information to the military force from its vantage point and interactions with international, regional, and local civilian organizations and civil government.

CA performs an important liaison function between the military force and the local civil authorities and IOs, NGOs, and PVOs established in the Area of Operations. CA provides the commander the means to shape his battlespace in regards to these significant actors, and to synchronize their actions with those of the military force.

CA assists the military force in anticipating, facilitating, coordinating, and orchestrating those civil-military functions and activities pertaining to the civilian population, government, and economy in the AO where the activities of the military force and the collection of supporting IOs, NGOs, and PVOs overlap.[162] Civil Affairs personnel ensure that the civil-military functions undertaken are linked to the operational objectives of the military force.[163] Once the military force has created and sustained the necessary pre-conditions for effective civil governance, CA, through its liaison with civil authorities, IOs, NGOs, and PVOs, supports the successful transition from military operations to a self-sustaining peace maintained by those civil organizations and agencies who will remain active long afterwards and who will achieve the ultimate desired end state.[164]

CA build public support for the military force and its objectives, which affects the legitimacy of supporting political institutions and the political underpinnings of the peace operation itself.[165] By building public support for the military force, CA reduces the threat from acts of civil disobedience and civil disturbances, and enhances force protection. CA personnel publicize CA activities to leverage their effects beyond the immediate audience. By exploiting existing local media through press conferences, talk shows, local newspapers, and by leveraging their participation in forums of civilian governmental leaders, CA foster support for, or at the very least, tolerance of, the military force and its mandate.[166] In OJE, OJG and OJF, CA units were tasked to publicize their activities in the local and international press, as well as to provide information to aid the local population in the form of civil information.[167]

In providing civil-military information to the civilian leadership and population, CA personnel must be certain to reinforce the established Information Campaign themes to ensure consistency and unity of effort throughout all axes of the information campaign. Civil Affairs is particularly important to information operations because CA activities involve influencing or controlling indigenous infrastructure and interface with key organizations and individuals.[168] CA, PSYOP, and PA elements are able to use the same communications media with essentially the same messages but to different audiences. CA and PSYOP address local populations, while PA personnel address friendly forces and national and international news media. PA, PSYOP, and CA all communicate information to critical audiences to influence their understanding and perception of the operation. Planning and execution of the information campaign across the three disciplines **"must be synchronized, and the messages they communicate must be truthful and mutually supportive to ensure that credibility is not undermined."**[169] A coordinated IO plan incorporating both PA and CA is critical for building legitimacy for host nation, coalition, U.S. and world support – especially in MOOTW.[170]

CA provide a collection means for the commander to collect CCIR through their liaison and interaction with local civil authorities and IOs, NGOs, and PVOs in the AO.[171] In peace operations, the CCIR are often obtained through other-than-the-conventional information-gathering entities. CA information gathering activities in peace operations encompass the complete spectrum of cultural, social, political, and economic issues within the AO to provide the commander his information requirements in these areas, primarily in the form of HUMINT.[172] In conducting information-gathering activities, however, CA personnel shall avoid appearing to be intelligence agents, or risk degradation of their primary mission.[173] In OJE, OJG and OJF, CA personnel enjoyed greater freedom of movement on the battlefield as they were excepted from the four-vehicle convoy rule and could travel in two-vehicle convoys. This facilitated their ability to both gather and disseminate information.

CA liaison with key audiences provides opportunities for message dissemination.

Civil-Military Information Supports Information Campaign.

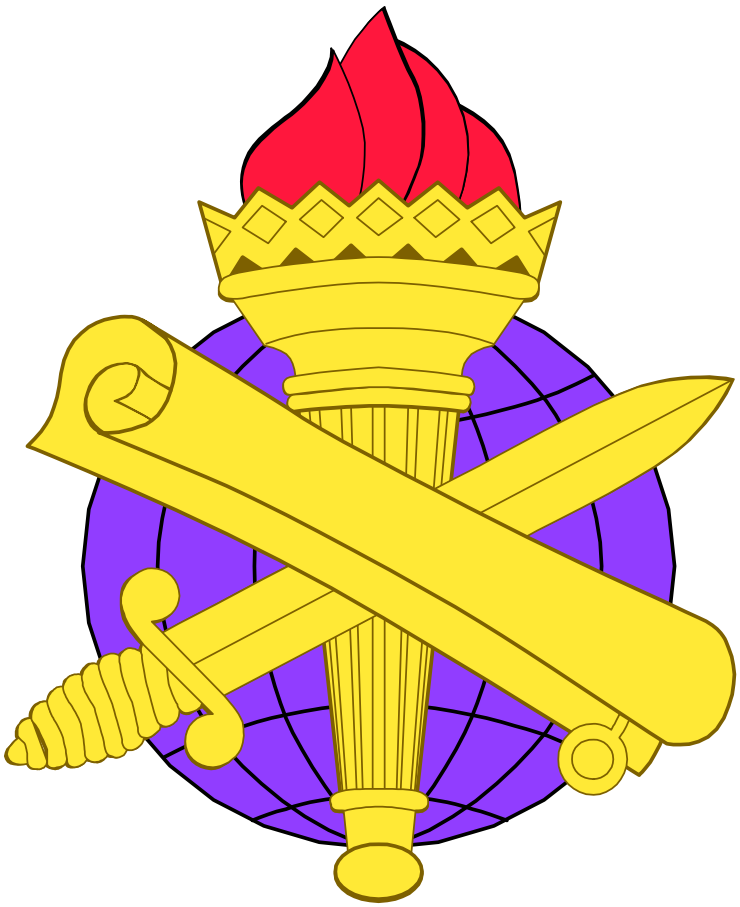
Civil Affairs in peace operations include civil-military information programs designed to inform the local populace about on-going military operations to secure their acquiescence and non-interference. An example of such an operation was the mine-awareness puppet show presented to Bosnian children in Multi-National Division-North AO. TFE CA produced a puppet show that was shown to children throughout BiH. The Coalition Press Information Center provided publicity. The CA unit supporting TFE used volunteer soldiers to present the puppet show with the assistance of interpreters.[174] The puppet shows were given to local school children in groups as large as 100. The puppets represented people of different color and ethnic backgrounds. Themes focused on people of diversity living in peace and harmony. The puppet show was very popular with the children who seemed to understand and accept the moral lessons the show presented. An additional benefit was that the puppet show provided the opportunity for CA personnel to meet and talk to mayors and other local leaders, who otherwise would have been inaccessible.[175]

Another example of Civil-Military Information Operations supporting IO is found in the spin-off effects of the routine liaison with local civilian officials. Civil Affairs Direct Support Team (DST) Commanders routinely establish liaison with the leaders of the civilian communities in the unit's area of operations. These CA DST Commanders are presented with opportunities to address influencers and leaders of the community at official functions, and, in so doing, can reinforce Information Operations Campaign Themes. Current Information Operations doctrine recognizes that CA personnel provide valuable information and intelligence by performing **"liaison with key actors and influencers (and) with NGOs, PVOs, and civil authorities."**[176] Doctrine further states, that **"the nature of CA activities and the need for CA personnel to develop and maintain a close relationship with the civilian populace puts them in a favorable position to gather information."**[177] However, not addressed is the ability of CA personnel to support the Information Operations Campaign Themes.[178]

The CA officer is the point of contact for civil-military cooperation between the friendly force and the local communities. After a period of successful interaction with local leaders, the CA officer is likely to be treated as an honored guest as the official representative of the U.S. or Coalition force and will likely be invited to attend official functions and community activities. It is on these occasions where the CA officer may be called upon to say a few words on behalf of the U.S. or Coalition force.

In July 1997, a CA DST Commander who regularly worked with the mayor of the town outside the base camp was invited to attend the dedication of a memorial in the town square. Being the senior representative of SFOR on the scene, he was asked to say a few words on what was a very solemn and very significant event for the people of the town. Local media were on hand to capture the event, and, potentially, to broadcast or print the remarks of the DST Commander throughout the region. Being knowledgeable of the SFOR Information Campaign themes, the DST Commander was able to confidently give a short speech which both reinforced the IO Campaign Themes and strengthened the working relationship between SFOR and the community.

Civil Affairs DST Commanders routinely liaison and interact with local officials while conducting civil-military cooperation. In the course of those duties, DST commanders may be called upon to speak on behalf of the U.S. or Coalition force to an audience of community influencers and leaders, or to an assembly of the community's citizens. The remarks made at such occasions will either re-enforce or degrade the objectives of the IO Campaign. Therefore, CA DST Commanders must be thoroughly familiar with Information Operations Campaign Themes to reinforce those themes when interacting with local communities.✪



Endnotes, Chapter Three

[1] See Office of the Chairman of the Joint Chiefs of Staff (CJCS), ***Command and Control Warfare,*** **Joint Publication 3-13.1,** (Washington, DC, USGPO), 7 February 1996, p. J-5. The term "co-opt" means to appropriate as one's own.
[2] Center for Army Lessons Learned, ***Initial Impressions Report - Operation JOINT ENDEAVOR – Task Force Eagle Initial Operations,*** (Unclassified, Distribution Limited, Fort Leavenworth, KS: CALL), May 1996, p. 61.
[3] Headquarters, U.S. Army Training and Doctrine Command, ***Force XXI Operations,*** **TRADOC PAM 525-5,** Fort Monroe, VA, 1 August 1994, Chapter 3.
[4] Headquarters, Dept. of the Army, ***Information Operations,*** **Field Manual 100-6,** op. cit., p. 3-0.
[5] Ibid., p. 4-3.
[6] CJCS, ***Joint Doctrine for Command and Control Warfare,*** **Joint Publication 3-13.1,** op. cit., p. v.
[7] Headquarters, Department of the Army, ***Intelligence and Electronic Warfare Operations,*** **Field Manual 34-1,** (Washington, DC: USGPO), 27 September 1994, p. 7-4.
[8] Office of the Chairman of the Joint Chiefs of Staff, ***Information Warfare - A Strategy for Peace...The Decisive Edge in War,*** (Washington, DC: USGPO), 1996, p. 13.
[9] CJCS, ***Command and Control Warfare,*** **Joint Publication 3-13.1,** (Washington, DC: USGPO), 7 February 1996, p. v.
[10] CJCS, ***Joint Doctrine for Command and Control Warfare,*** op. cit., p. J-5.
[11] Headquarters, Department of the Army, ***Battlefield Deception,*** **Field Manual 90-2,** (Washington, DC: USGPO), 3 October 1988., p. 2-1. Although this manual is now obsolete, there is no follow-on Deception Manual yet published. Deception will be covered in the next edition of **Field Manual 100-6, *Information Operations.***
[12] Maj. Gen. David L. Grange, U.S. Army, and Col. James A. Kelley, U.S.Army, **"Information Operations for the Ground Commander,"** op. cit., p. 9.
[13] Headquarters, Dept. of the Army, ***Psychological Operations,*** **Field Manual 33-1,** (Unclassified, Distribution Limited), (Washington, DC: USGPO), 18 February 1993, p. 3-6.
[14] See Stephen D. Brown, **"PSYOP in Operation UPHOLD DEMOCRACY,"** ***Military Review,*** Vol. LXXVI, No. 5, September-October 1996, p. 57.
[15] See Jeffrey P. Jones and Michael P. Mathews, **"PSYOP and the Warfighting CINC,"** ***Joint Forces Quarterly,*** No. 8, Summer 1995, p. 31.
[16] Headquarters, Dept. of the Army, ***Peace Operations,*** **Field Manual 100-23,** op. cit., p. 40.
[17] Headquarters, Dept. of the Army, ***Psychological Operations,*** **Field Manual 33-1,** (Unclassified, Distribution Limited, Washington, DC: USGPO), 18 February 1993, p. 3-28.
[18] Office of the Chairman of the Joint Chiefs of Staff, ***Joint Doctrine for Psychological Operations,*** **Joint Pub 3-53,** (Washington, DC: USGPO), 10 July 1996, p. V-2.
[19] Headquarters, Dept. of the Army, ***Psychological Operations,*** **Field Manual 33-1,** (Unclassified, Distribution Limited, Washington, DC: USGPO), 18 February 1993, pp. 1-3 and 3-9.
[20] Ibid, p. 3-25
[21] Office of the Chairman of the Joint Chiefs of Staff, ***Joint Doctrine for Psychological Operations,*** **Joint Pub 3-53,** (Washington, DC: USGPO), 10 July 1996, p. II-5.
[22] Stephen D. Brown, **"PSYOP in Operation UPHOLD DEMOCRACY,"** ***Military Review,*** Vol. LXXVI, No. 5, September-October 1996, p. 60.
[23] Office of the Chairman of the Joint Chiefs of Staff, ***Joint Doctrine for Psychological Operations,*** **Joint Pub 3-53,** op. cit., p. IV-4.
[24] Ibid., p. IV-7.
[25] Ibid.
[26] Ibid., p. V-1.
[27] Larry K. Wentz, National Defense University, CCRP, ***Information Operations: The IFOR Experience,*** National Defense University, Command and Control Research Program, p. 18, downloaded 19 January 1999 from http://www.dodcrp.org/bo_infoop1.html.
[28] Headquarters, Dept. of the Army, ***Psychological Operations,*** **Field Manual 33-1,** (Unclassified, Distribution Limited), (Washington, DC: USGPO), 18 February 1993, p. 1-2.

[29] William B. Buchanan, ***U.S. European Command Support of Operation JOINT GUARD (21 December 1996 - 20 December 1997),*** (Unclassified, Distribution Limited, Alexandria, VA: Institute for Defense Analysis), IDA Paper P-3389, 1998, p. III-25.
[30] Pascale Combelles Siegel, ***Target Bosnia: Integrating Information Activities in Peace Operations,*** Command and Control Research Program, National Defense University, (Washington, DC: NDU Press), 1998, p. 99.
[31] Headquarters, Dept. of the Army, ***Psychological Operations,*** **Field Manual 33-1,** (Unclassified, Distribution Limited, Washington, DC: USGPO), 18 February 1993, p. 1-3.
[32] Office of the Chairman of the Joint Chiefs of Staff, ***Joint Doctrine for Psychological Operations,*** **Joint Pub 3-53,** (Washington, DC: USGPO), 10 July 1996, p. I-8.
[33] See Office of the Chairman of the Joint Chiefs of Staff, *Joint Doctrine for Command and Control Warfare*, op. cit., p. II-4. See also Headquarters, Training and Doctrine Command, ***Concept for Information Operations,*** **TRADOC Pamphlet 525-69,** (Fort Monroe, VA: TRADOC), 1 August 1995, p. 16.
[34] Headquarters, Dept. of the Army, ***Psychological Operations,*** **Field Manual 33-1,** (Unclassified, Distribution Limited), (Washington, DC: USGPO), 18 February 1993, p. 3-9.
[35] Headquarters, Dept. of the Army, ***Information Operations,*** **Field Manual 100-6,** (Washington, DC: USGPO), 27 August 1996, p. 5-5.
[36] Ibid, p. 3-7.
[37] Ibid, p. 3-5.
[38] In those areas occupied by the Bosnian Serbs, IFOR soldiers were the targets of an information campaign that was already in full operation when the IFOR troops arrived. According to Mr. Larry Wentz, "...the IFOR Information Campaign (IIC) was at a disadvantage at the outset because it had to compete immediately with an already established and effective campaign that could get inside of the IFOR decision loop and outmaneuver some of the initial IFOR efforts." Larry K. Wentz, ed., ***Lessons from Bosnia: The IFOR Experience,*** Command and Control Research Program, National Defense University, (Washington, DC: NDU Press), 1998, p. 65.
[39] Center for Army Lessons Learned, ***B/H CAAT2, Initial Impressions Report – Operation JOINT ENDEAVOR – Continuing Operations,*** (Unclassified, Distribution Limited, Fort Leavenworth, KS: CALL), September 1996, p. 80.
[40] See Deede Doke, **"Radio Team Broadcasts Message of Peace,"** ***Stars and Stripes,*** Vol. 56, No. 89, 15 July 1997, p. 17.
[41] Office of the Chairman of the Joint Chiefs of Staff, ***Joint Doctrine for Psychological Operations,*** **Joint Pub 3-53,** (Washington, DC: USGPO), 10 July 1996, p. III-6.
[42] Stephen D. Brown, **"PSYOP in Operation UPHOLD DEMOCRACY,"** ***Military Review,*** Vol. LXXVI, No. 5, September-October 1996, p. 61.
[43] Associated Press, **"Planes Sent to Silence Serb Rhetoric,"** ***The Kansas City Star,*** 12 September 1997, p. A-5.
[44] Jeffrey P. Jones, and Michael P. Mathews, **"PSYOP and the Warfighting CINC,"** ***Joint Forces Quarterly,*** Summer 1995, No. 8, pp. 28-33. See also Office of the Chairman of the Joint Chiefs of Staff, ***Joint Doctrine for Psychological Operations,*** **Joint Pub 3-53,** (Washington, DC: USGPO), July 1993, p. A-2.
[45] See Tracy Wilkinson, **"Trying to Extract War From Journalism,"** ***The Los Angeles Times,*** Sunday, October 26, 1997, p. 12A. One PSYOP officer remarked that since most Bosnians had little knowledge of Anglo-American politicians and philosophers from history, the leaflet would have been more effective if relevant quotations from more well-known regional figures had been used.
[46] William B. Buchanan, ***U.S. European Command Support of Operation JOINT GUARD (21 December 1996 - 20 December 1997),*** (Unclassified, Distribution Limited, Alexandria, VA: Institute for Defense Analysis), IDA Paper P-3389, 1998, p. A-4.
[47] Ibid.
[48] Center for Army Lessons Learned, ***B/H CAAT XI Initial Impressions Report***, (Unclassified, Distribution Limited, Fort Leavenworth, KS: CALL), April 1998, p. 6.
[49] This section was originally published as CALLCOMS Observation 10008-93025 in ***B/H CAAT IX Initial Impressions Report,*** (Unclassified, Distribution Limited), op. cit., March 1998, pp. A-99 to A-101.
[50] One of the first challenges to the PSYOP mission was gaining access to the most reliable and capable print facility for publishing a high-quality product. The PSYOP forces from home station assumed that they would have access to the best machinery at the Rodelheim Print Plant. Unfortunately, when a real-world mission emerged, they

discovered that the only printers they could access were antiquated Heidelberg Presses, which could print neither high quantity nor quality. Speed and an attractive appearance were viewed as essential to mission success. By January 1996, when the third edition of the HOP was published, the CJICTF contracted with a publishing company in Zagreb, Croatia. This contract lasted for three months. The quality and speed of production at this facility greatly enhanced the CJICTF's ability to disseminate their messages. For political and economic reasons, the CJICTF deployed a Modular Print System (MPS) to Sarajevo. This system produced several editions of the *Herald of Peace* and innumerable posters and handbills. The final editions of the paper were published by OKO Printers, as were the initial editions of the ***Herald of Progress.***

[51] The CJICTF decided to produce articles in both Latinic and Cyrillic. One half of the periodical was in one alphabet, the other half in the other. They were essentially and technically two different papers in one. One half of the paper was for Bosniacs and Croats, while the other side was for Serbs. This format allowed only eight pages of information in a 16-page periodical.

[52] The driving force for having products printed in Bosnia was the initiative, consistent with PSYOP doctrine and U.S. protocols, to patronize local economies through contracting with local companies. The inclusion to this program of a protocol with a publishing company in Banja Luka, Republika Srpska (RS) spread money to a Serb company. This reinforced SFOR's directive to be even-handed and having the collateral benefit of circumventing inactivity by some elements in SFOR in disseminating products by having the publisher distribute copies to kiosks in the RS.

[53] Headquarters, Training and Doctrine Command, ***Concept for Information Operations,*** **TRADOC Pamphlet 525-69,** (Fort Monroe, VA), 1 August 1995, p. 9.

[54] Les Aspin, ***Annual Report to the President and the Congress*****,** (Washington, DC: USGPO), January 1994, p. 244.

[55] Headquarters, Dept. of the Army, ***Information Operations,*** **Field Manual 100-6,** op. cit., p. 3-5.

[56] Struble, Dan, Lt. Cdr., USNR, "**What Is Command and Control Warfare?"** ***Naval War College Review,*** Summer 1995, Vol. XLVIII, No. 3, p. 91.

[57] Headquarters, Dept. of the Army, ***Information Operations,*** **Field Manual 100-6,** op. cit., p. 3-5.

[58] See Center for Army Lessons Learned, Initial Impressions Report, ***Operation JOINT ENDEAVOR, Bosnia-Herzegovina, Task Force Eagle Initial Impressions*****,** (Unclassified, Distribution Limited, Fort Leavenworth, KS: CALL), May 1996, p. 61.

[59] Larry K. Wentz, ed., ***Lessons From Bosnia: The IFOR Experience,*** Command and Control Research Program, National Defense University, (Washington, DC: NDU Press), 1998, p. 23.

[60] Lawrence E. Caspar, Irving L. Halter, Earl W. Powers, Paul J. Selva, Thomas W. Steffens, and T. Lamar Willis, **"Knowledge-Based Warfare: A Security Strategy for the Next Century,"** ***Joint Forces Quarterly,*** Autumn 1996, No. 13, p. 85.

[61] Headquarters, Dept. of the Army, ***Peace Operations,*** **Field Manual 100-23,** (Washington, DC: USGPO), 30 December 1994, p. 17.

[62] Associated Press, **"NATO Pulls Plug on Serb Telecast,"** ***The Kansas City Star,*** October 19, 1997, p. A14.

[63] Pascale Combelles Siegel, ***Target Bosnia: Integrating Information Activities in Peace Operations,*** (Command and Control Research Program, National Defense University, Washington, DC: NDU Press), 1998, pp. 160 and 161.

[64] See Tracy Wilkinson, **"Trying to Extract War from Journalism,"** ***Los Angeles Times***, Sunday, October 26, 1997, p. 12A.

[65] See Center for Army Lessons Learned, ***B/H CAAT Elections, Initial Impressions Report*** (Unclassified, Distribution Limited, Fort Leavenworth, KS: CALL), March 1998, p. 83.

[66] Larry K. Wentz, *IFOR* ***C 4ISR Experiences,*** a report prepared for the National Defense University, Command and Control Research Program, p. 5. See the CCRP Website at http://www.dodccrp.org/bosnia.htm#REPORTS/BRIEFINGS.

[67] Philip Shenon, **"U.S. and Allies Plan to Curb Bosnian Propaganda,"** ***The New York Times,*** 24 April 1998.

[68] William B. Buchanan, ***U.S. European Command Support of Operation JOINT GUARD (21 December 1996 - 20 December 1997),*** (Unclassified, Distribution Limited, Alexandria, VA: Institute for Defense Analysis), IDA Paper P-3389, 1998, p. IV-15.

[69] Dennis Steele, **"Hill 562: Boots in the Mud,"** ***Army,*** Vol. 48, No. 1, January 1998, pp. 39-41.

[70] See SGT Jerry Parisellad, **"Broadcasts of Violence Stop with SFOR Help,"** 362d Military Public Affairs Detachment, Task Force Eagle ***Talon,*** Vol. 3, No. 40, October 10, 1997, Eagle Base, Tuzla, Bosnia.
[71] Dennis Steele, op. cit. p. 41.
[72] Press Release, Multi-National Division-North, Coalition Press Information Center, Operation JOINT GUARD, Release No. 0828-3, p. 1.
[73] Asst. Chief of Staff, G-2, 1st Infantry Division, ***Tuzla Night Owl,*** Vol. 2, Issue 241, August 29, 1997, Eagle Base, Bosnia, p. 1.
[74] See Jerry Merideth, **"They Got Me Good, GI Relates,"** ***The Stars and Stripes,*** Vol. 56, No. 134, August 29, 1997, pp. 1 and 4.
[75] SGT Mark Schulz and PFC Todd Edwards, 372d Mobile Public Affairs Detachment, **"Rioters: Soldiers React to Civil Unrest,"** ***Talon,*** Vol. 3, No. 36, 05 September 1998.
[76] Headquarters, Dept. of the Army,***Information Operations,*** **Field Manual 100-6,** op. cit., p. 2-4, emphasis added.
[77] Ibid. p. 3-5. Physical destruction is defined as "The application of combat power to destroy or *neutralize* enemy forces and installations," (emphasis added).
[78] MND-N, CPIC, OJG, Press Release No. 0828-5, Eagle Base, Bosnia, 28 August 1997.
[79] Military Operations on Urbanized Terrain. For information on MOUT, see Field Manual 90-10-1, Headquarters, Dept. of the Army, (Washington, DC: USGPO), 12 May 1993, and Field Manual 90-10, Headquarters, Dept. of the Army, (Washington, DC: USGPO), 15 August 1979.
[80] Headquarters, Dept. of the Army, ***Intelligence and Electronic Warfare Operations,*** **Field Manual 34-1,** op. cit., p. 2-21.
[81] Headquarters, Dept. of the Army, ***Division Operations,*** **Field Manual 71-100** (Washington, DC: USPO), 28 August 1996, p. 2-13. See also Office of the Chairman of the Joint Chiefs of Staff, ***Information Warfare - A Strategy for Peace....The Decisive Edge in War,*** op. cit., p. 13.
[82] William W. McCollum, **"The Role of the Intelligence Community in Preparing to Win the Information War,"** a strategy research report submitted to the faculty of the U.S. Army War College, Carlisle Barracks, PA, 10 April 1997, pp. 12-13.
[83] Headquarters, Training and Doctrine Command, ***Concept for Information Operations,*** **TRADOC Pamphlet 525-69,** op. cit., p. 9.
[84] Headquarters, Dept. of the Army, ***Decisive Force: The Army in Theater Operations,*** **Field Manual 100-7,** op. cit., p. 8-3.
[85] William B. Buchanan, ***U.S. European Command Support of Operation JOINT GUARD (21 December 1996 - 20 December 1997),*** (Unclassified, Distribution Limited, Alexandria, VA: Institute for Defense Analysis), IDA Paper P-3389, 1998, p. A-8
[86] Headquarters USAREUR, ***Operation JOINT ENDEAVOR, USAREUR Headquarters After-Action Report,*** May 1997, pp. 75 and 88.
[87] Headquarters, Dept. of the Army, ***Peace Operations,*** **Field Manual 100-23,** 30 December 1994, op. cit., p. 39.
[88] Headquarters, Dept. of the Army, ***Tactics, Techniques and Procedures for the Remotely Monitored Battlefield Sensor System (REMBASS),*** **Field Manual 34-10-1,** 18 June 1991, does not specifically address employment of REMBASS or Improved-REMBASS (I-REMBASS) in a peace operations environment.
[89] Martin C. Libicki, **"DBK and Its Consequences,"** in ***Dominant Battlespace Knowledge,*** Stuart E. Johnson and Martin C. Libicki, Eds., (The Center for Advanced Concepts and Technology, National Defense University, Washington, DC: NDU Press), revised edition, April 1996, pp. 40-41.
[90] Headquarters, USAREUR, ***Operation JOINT ENDEAVOR, USAREUR Headquarters After-Action Report,*** op. cit., p. 198.
[91] Ibid.
[92] Office of the Chairman of the Joint Chiefs of Staff, ***Joint Publication 3-54, Joint Doctrine for Operations Security,*** Washington, DC, 24 January 1997, p. 1-1.
[93] Office of the Chairman of the Joint Chiefs of Staff, ***Joint Doctrine for Information Operations,*** **Joint Publication 3-13,** 9 October 1998, p. II-4.
[94] Headquarters, Department of the Army, ***Division Operations,*** **Field Manual 71-100,** June 1990, p. 3-14. The 1996 version is not as specific, but the process outlined on page 30 is consistent with that in Headquarters, Dept. of the Army, ***Staff Organization and Operations,*** **Field Manual 101-5,** p. 4-13.

[95] Headquarters, Dept. of the Army, ***Decisive Force: The Army in Theater Operations,*** **Field Manual 100-7,** op. cit., p. 8-3.
[96] Office of the Chairman of the Joint Chiefs of Staff, **Joint Publication 3-54,** ***Joint Doctrine for Operations Security,*** op. cit., p. vi.
[97] Interagency OPSEC Support Staff, ***National Operations Security Doctrine,*** (Greenbelt, MD: USGPO), January 1993, p. 2.
[98] The operating concept of transparency in peace operations, and its relationship to security is addressed in Headquarters, Dept. of the Army, ***Peace Operations,*** **Field Manual 100-23,** (Washington, DC: USGPO, 30 December 1994), p. 17.
[99] Gary E. Phillips, Col., U.S. Army, ***Information Operations - A New Tool for Peacekeeping,*** a monograph submitted to the U.S. Army Command and General Staff College, School for Advanced Military Studies, Fort Leavenworth KS, 22 May 1998, p. 40.
[100] Headquarters, TRADOC, ***The Army in Theater Operations,*** **Field Manual 100-7,** Coordinating Draft, 24 December 1991, p. 5-5. Oddly, the specific linkage between OPSEC and PA is not mentioned in the 1995 manual.
[101] Headquarters, Dept. of the Army, ***Peace Operations,*** **Field Manual 100-23,** op. cit., p. 36.
[102] CJCS, ***Command and Control Warfare,*** **Joint Pub 3-13.1,** op. cit., p. II-2.
[103] **Center for Army Lessons Learned Newsletter No. 97-1,** ***Tactics, Techniques, and Procedures from Operation JOINT ENDEAVOR,*** (Unclassified, Distribution Limited), Fort Leavenworth, KS: CALL, January 1997, p. 46.
[104] Kenneth Allard, **"Information Operations in Bosnia: A Preliminary Assessment,"** Chapter X in ***Lessons from Bosnia: The IFOR Experience,*** Larry K. Wentz, ed. (Washington, DC: NDU Press, January 1998), p. 268.
[105] Brian E. Fredericks, Col., U.S. Army, **"Information Warfare at the Crossroads,"** ***Joint Forces Quarterly,*** Summer 1997, No. 16, p. 101.
[106] Gary E. Phillips, Col., U.S. Army, ***Information Operations – A New Tool for Peacekeeping,*** a monograph submitted to the U.S. Army Command and General Staff College, School of Advanced Military Studies, Fort Leavenworth, KS, 22 May 1997, p. 41. See also **Field Manual 100-23,** ***Peace Operations,*** op. cit., p. 36.
[107] Headquarters, Dept. of the Army, ***Peace Operations,*** **Field Manual 100-23,** op. cit., p. 36.
[108] Ibid. Army Force Protection policies are explained in **AR 525-13,** ***Force Protection.*** The pillars of force protection listed in the Army regulation are: OPSEC, Personal Security, Law Enforcement, and Counter-Terrorism/Anti-Terrorism programs.
[109] Joint Warfighting Center, ***Joint Task Force Commander's Handbook for Peace Operations,*** Fort Monroe, VA, 28 February 1995, p. 55.
[110] Office of the Chairman of the Joint Chiefs of Staff, ***Joint Doctrine for Information Operations,*** **Joint Publication 3-13,** 9 October 1998, pp. III-3 and III-4.
[111] Headquarters, Dept. of the Army, ***Doctrine for Army Special Operations Forces,*** **Field Manual 100-25,** Washington, DC: USGPO (Unclassified, Distribution Limited), 12 December 1991, p. 13-5.
[112] Headquarters, Dept. of the Army, **Field Manual 34-60,** ***Counterintelligence,*** Washington, DC, 3 October 1995, Chapter 4.
[113] Office of the Chairman of the Joint Chiefs of Staff, ***Joint Doctrine for Information Operations,*** **Joint Publication 3-13,** 9 October 1998, p. III-7.
[114] Center for Army Lessons Learned, ***B/H CAAT IX Initial Impressions Report,*** (Unclassified, Distribution Limited), Fort Leavenworth, KS: CALL, April 1998, p. A-17.
[115] Headquarters, Department of the Army, ***Battlefield Deception,*** **Field Manual 90-2,** op. cit., p. 1-33.
[116] Headquarters, Dept. of the Army, **Army Regulation 530-1,** ***Operations Security (OPSEC),*** (Washington, DC: USGPO, Unclassified, Distribution Limited), March 1995.
[117] Headquarters, Dept. of the Army, ***Battlefield Deception,*** **Field Manual 90-2,** op. cit., p. 1-0.
[118] Headquarters, Dept. of the Army, ***Peace Operations,*** **Field Manual 100-23,** op. cit., p. 37.
[119] Headquarters, Dept. of the Army, ***Decisive Force, The Army in Theater Operations,*** **Field Manual 100-7,** op. cit., 31 May 1995, p. 8-13.
[120] Office of the Chief of Staff of the Air Force, Draft Air Force Operational Doctrine Manual, ***Information Operations,*** AFDD 2-5, December 1997, p. 11 (the 5 August 1998 edition does not specifically mention PA and merely directs commanders to coordinate deception operations with "their senior commander," p. 14). See also, HQ

TRADOC, ***The Army in Theater Operations,*** 24 December 1991, Coordinating Draft of FM 100-7, which makes this association on p. 5-5. See also, Office of the Chairman of the Joint Chiefs of Staff, ***Joint Doctrine for Military Deception,*** **Joint Publication 3-58,** Washington, DC, 31 May 1996, pp. v and I-4, which discuss the necessary coordination and relationship between PA and military deception.

[121] Headquarters, Department of the Army, ***Decisive Force: The Army in Theater Operations,*** **Field Manual 100-7,** op. cit., p. 8-3.

[122] Larry K. Wentz, ***Information Operations: The IFOR Experience,*** op. cit., p. 11.

[123] Pascale Combelles Siegel, ***Target Bosnia: Integrating Information Activities in Peace Operations,*** Command and Control Research Program, National Defense University (Washington, DC: NDU Press), 1998, p. 117.

[124] Headquarters, Dept. of the Army, ***The Army in Multinational Operations,*** **Field Manual 100-8,** op. cit., p. 3-15.

[125] Headquarters, Dept. of the Army, ***Battlefield Deception,*** **Field Manual 90-2,** op. cit., p. 1-2.

[126] HQDA, ***Military Operations in Low-Intensity Conflict,*** **Field Manual 100-20** (Washington, DC: USGPO), 5 December 1990, p. 4-7.

[127] Office of the Chairman of the Joint Chiefs of Staff, ***Joint Doctrine for Information Operations,*** **Joint Publication 3-13,** op. cit., p. II-4.

[128] Headquarters, Dept. of the Army, ***Battlefield Deception,*** **Field Manual 90-2,** op. cit., p. 1-9.

[129] Michael R. Gordon and General Bernard E. Trainor, ***The General's War*** (Boston: Little Brown and Company), 1991, p. 294.

[130] Headquarters, Department of the Army, ***The Army in Theater Operations,*** **Field Manual 100-7,** pp. 7-22 and 3-8.

[131] Headquarters, Dept. of the Army, ***Corps Operations,*** **Field Manual 100-15,** (Washington, DC: USGPO), 13 September 1989, p. 4-25.

[132] Headquarters, Dept. of the Army, ***Peace Operations,*** **Field Manual 100-23,** op. cit., p. 47.

[133] HQ, TRADOC, Information Operations Division, Brochure, ***Information Operations,*** (Fort Monroe, VA: TRADOC), 22 January 1997, p. 7.

[134] Brian E. Fredericks, Col., U.S. Army, **"Information Warfare at the Crossroads,"** ***Joint Forces Quarterly,*** Summer 1997, No. 16, pp. 97-103.

[135] Headquarters, Dept. of the Army, ***Information Operations,*** **Field Manual 100-6,** op. cit., p. 3-14.

[136] Dennis M. Murphy, Lt. Col., U.S. Army, **"Information Operations on the Nontraditional Battlefield,"** ***Military Review,*** Vol. LXXVI, No. 6, November-December 1996, p. 9.

[137] While PA operations which provide news and information are proactive and, therefore, offensive in nature, C^2-Protect can be offensive or defensive, see Headquarters, Dept. of the Army, ***Information Operations,*** **Field Manual 100-6,** op. cit., p. 3-9.

[138] Erin Gallogly-Staver, Maj., U.S. Army, and Raymond S. Hilliard, Maj., U.S. Army, **"Information Warfare: Opposing Force (OPFOR) Doctrine -- An Integrated Approach,"** ***News from the Front!***, Center for Army Lessons Learned, Fort Leavenworth, KS, September-October 1997, p. 15.

[139] Ronald T. Sconyers, Col., U.S. Air Force, **"The Information War,"** ***Military Review,*** Vol. LXIX, No. 2, February 1989, p. 48.

[140] Headquarters, Dept. of the Army, ***Peace Operations,*** **Field Manual 100-23,** op. cit., p. 48.

[141] Headquarters, Dept. of the Army, ***Psychological Operations,*** **Field Manual 33-1,** (Unclassified, Distribution Limited), op. cit., p. 2-2.

[142] Headquarters, Dept. of the Army, ***Information Operations,*** **Field Manual 100-6,** op. cit., p. 3-14.

[143] Headquarters, Dept. of the Army, ***Peace Operations,*** **FM 100-23,** op. cit., p. 48.

[144] Headquarters, Training and Doctrine Command, ***Concept for Information Operations,*** **TRADOC Pamphlet 525-69** (Fort Monroe, VA: TRADOC), 1 August 1995, p. 14.

[145] For an overview of PA missions, see ***Information Operations,*** **Field Manual 100-6,** op. cit., Figure 3-5, and Coordination and Support tasks on page 3-15.

[146] Headquarters, Dept. of the Army, ***Peace Operations,*** **Field Manual 100-23,** op. cit., p. 48.

[147] Center for Army Lessons Learned, ***B/H CAAT 2 Initial Impressions Report - Operation JOINT ENDEAVOR – Task Force Eagle Continuing Operations,*** (Unclassified, Distribution Limited, Fort Leavenworth, KS: CALL), September 1996, p. 33.

[148] Allard, Kenneth, **"Information Operations in Bosnia: A Preliminary Assessment,"** Chapter X in ***Lessons from Bosnia: The IFOR Experience,*** Larry K. Wentz, ed. (Washington, DC: NDU Press, January 1998), p. 268.
[149] Headquarters, USAREUR, ***Operation JOINT ENDEAVOR After-Action Report,*** May 1997, pp. 239-240.
[150] Headquarters, Dept. of the Army, ***Information Operations,*** **Field Manual 100-6,** op. cit., p. 2-5.
[151] United Nations International Police Task Force, Office of the Commisioner, Policy of Local Police Checkpoints, May 1997.
[152] See Srecko Latal, **"Serbian Official Alleges Brutality by U.S. Soldiers,"** ***Stars and Stripes,*** Vol. 56, No. 71, 27 June 1997, pp. 1 & 4.
[153] See Chuck Roberts, **"Colonel Denounces Serbian Claims,"** ***Stars and Stripes,*** Vol. 56, No. 72, 28 June 1997, pp. 1 & 2.
[154] Armed Forces Press Report issued 031445 GMT by HQ SFOR, Sarajevo, Bosnia.
[155] Headquarters, Dept. of the Army, ***Information Operations,*** **Field Manual 100-6,** op. cit. p. 3-4.
[156] Headquarters, USAREUR, ***Operation JOINT ENDEAVOR, USAREUR Headquarters After-Action Report,*** op. cit., p. 245.
[157] Ibid., pp. 237 and 241.
[158] Center for Army Lessons Learned, ***In the Spotlight, Media and the Tactical Commander,*** **Newsletter No. 92-7,** December 1992, p. 3.
[159] Center for Army Lessons Learned, ***B/H CAAT 2 Initial Impressions Report - Operation JOINT ENDEAVOR – Task Force Eagle Continuing Operations,*** (Unclassified, Distribution Limited, Fort Leavenworth, KS: CALL), September 1996, p. 33.
[160] Ibid., p. C-65, CALLCOMS observation number 10000-85613.
[161] Ibid., p. C-64, CALLCOMS observation number 10001-58746.
[162] Headquarters, Dept. of the Army, ***The Army in Multinational Operations,*** **Field Manual 100-8,** op. cit., p. 2-19.
[163] For a description of the civil-military operations associated with CA and PSYOP in MOOTW, see Headquarters, Department of the Army, ***Military Operations in Low-Intensity Conflict,*** **Field Manual 100-20,** (Washington, DC: USGPO), 05 December 1990, p. 2-22.
[164] Headquarters, Dept. of the Army, ***Peace Operations,*** **Field Manual 100-23,** op. cit., p. 31.
[165] Pamela Brady, **"Joint Endeavor – The Role of Civil Affairs,"** ***Joint Forces Quarterly,*** Summer 1997, p. 47.
[166] Bruce Castka, **"The National Support Element in Hungary,"** ***Joint Forces Quarterly,*** Summer 1997, pp. 48-49. See also, Michael D. Starry, Col., U.S. Army, and Charles W. Anderson Jr., Lt. Col., U.S. Army, **"Field Manual 100-6: Information Operations,"** ***Military Review,*** November-December 1996, Vol. LXXVI, No. 6, p. 8.
[167] Pascale Combelles Siegel, ***Target Bosnia: Integrating Information Activities in Peace Operations,*** Command and Control Research Program, National Defense University (Washington, DC: NDU Press), 1998, p. 107.
[168] Brian E. Fredericks, Col., U.S. Army, **"Information Warfare at the Crossroads,"** ***Joint Forces Quarterly,*** Summer 1997, No. 16, p. 102.
[169] Headquarters, Dept. of the Army, ***Information Operations,*** **Field Manual 100-6,** op. cit., pp. 3-12 and 3-14.
[170] David L. Grange, Maj. Gen., U.S. Army, and James A. Kelley, Col., U.S. Army, **"Information Operations for the Ground Commander,"** ***Military Review,*** op. cit., p. 8. See also, Headquarters, Dept. of the Army, ***Peace Operations,*** **Field Manual 100-23,** op. cit., p. 18.
[171] Headquarters, Dept. of the Army, ***Information Operations,*** **Field Manual 100-6,** op. cit., p. 3-0.
[172] Headquarters, Dept. of the Army, ***Civil Affairs Operations,*** **Field Manual 41-10** (Unclassified, Distribution Limited, Washington, DC: USGPO), 11 January 1993, pp. 6-2 and 6-3.
[173] Ibid., p. 6-2.
[174] Multi-National Division-North, Coalition Press Information Center, Press Release Number: 0827-1 Date: 27 August 1997.
[175] Center for Army Lessons Learned, ***B/H CAAT XI, Initial Impressions Report*** (Unclassified, Distribution Limited, Fort Leavenworth, KS: CALL), April 1998, p. 12, CALLCOMS observation 10000-08008.
[176] Headquarters, Dept. of the Army, ***Information Operations,*** **Field Manual 100-6,** op. cit., p. 3-0.
[177] Ibid, p. 3-12.
[178] Except for one sentence in the Civil Affairs section of Chapter 3 of Field Manual 100-6, **"CA...personnel provide news and information to the local populace on the effects of combat operations,"** CA support to Information Operations Campaign Themes is not covered. See Field Manual 100-6, op. cit. p. 3-12.

Chapter Four
Relevant Information and Intelligence (RII)

"The main imperative guiding future operations, from full war to domestic support operations, will be to gain information and continued accurate and timely shared perceptions of the battlespace."[1]
-- TRADOC PAM 525-5, *Force XXI Operations*

Relevant information is defined as - "**Information drawn from the military information environment that significantly impacts, contributes to, or is related to the execution of the operational mission at hand."[2]** Intelligence is a subset of relevant information that focuses primarily upon foreign environments and identified existing and potential adversaries. In peace operations, the adversary is not merely the FWF political and military leadership and elements, but conditions and events that threaten the desired end state. In support of friendly operations, intelligence helps produce a common, current, and relevant picture of the battlespace that reduces uncertainty and shortens the commander's decisionmaking process.[3] This situational awareness, built from RII that can be shared throughout the force is referred to as the Relevant Common Picture (RCP). Access to the RCP contributes directly to effective C^2 during all stages of the decision and execution cycle at all levels of command.[4]

RII is collected in many ways: electronic, reconnaissance and reporting from the field, imagery, human intelligence, and from open sources. All soldiers are collectors of RII during peace operations. Soldiers must monitor everything that happens within range of observation, providing timely and accurate reports on every situation or incident that develops. Factual and impartial reporting constitutes the cornerstone of all successful peace operations. The use of maps, field sketches, diagrams, videotapes, pictures, and references to specific agreement or instructions contributes to the accuracy and utility of the RII provided.[5] Intelligence in peace operations may be referred to as ***information gathering,*** as the belligerent parties may perceive collecting intelligence as a hostile act. Just as PSYOP is known by other names in peace operations, the less innocuous term *information gathering* is less likely to damage the trust which the parties should have in the peace operations force that sustains legitimacy.[6]

"Peace operations often require augmentation of the intelligence staff." -- FM 100-23

Peace operations often require augmentation from higher headquarters. The size of the AO, the number of supported units, the nature of the threat, and the scope of the analytical effort required in a PKO or PEO environment are the reasons for augmentation. TFE was no exception. Thorough mission analysis and pre-deployment training identified the needs associated with the complex operating environment in Bosnia. This included increased HUMINT collection, the need for new, non-MTOE Signal Intelligence (SIGINT) capabilities, a near real-time Image Intelligence (IMINT) capability and increased analytical expertise.

The Military Intelligence Task Force (TF Lightning) was composed of units from several organizations.[7] The corps MI brigade provided the bulk of the augmentation, providing additional analytical personnel for the G2 Analysis and Control Element (ACE), CI/HUMINT teams, aerial exploitation and Long-Range Surveillance (LRS) teams. Other assets attached or in direct support of TFE from higher echelons included: Temporary Change-of Station-(TCS) personnel for key shortages, a National Intelligence Support Team (NIST), a G2X, Deployable Intelligence Support Element (DISE) teams, Allied Military Intelligence Battalion (AMIB) assets, Unmanned Aerial Vehicles (UAV), and liaison officers from theater agencies. TFE could leverage other theater and national assets through the NATO/Combined Air Operations Center collection management process. TFE also received sanctuary analytical and exploitation support from component, theater and national intelligence centers.

Several tailoring approaches were non-doctrinal, but successful, given the operating environment. Deployment of WARLORD-equipped theater mini-DISEs to multi-national maneuver units (Russian, Turk, NordPol Bdes) was key to connectivity and shared situational awareness.[8] The NIST, which is normally deployed at joint task force (JTF) level, was fully integrated into the division ACE. Since the bulk of the corps MI brigade deployed to TFE, the divisional MI battalion was attached to the MI brigade.

Intelligence Preparation of the Battlefield (IPB)

While the IPB process remains the same, the focus of intelligence and derived intelligence products are different in a MOOTW environment. The major differences include the impact of the political situation, to include such items as legal mandates or terms of reference, and the enormous demand for demographic analysis. New information categories will emerge for the commander as he directs troops and accomplishes missions in the MOOTW environment.[9] The nature of peace operations means that the IPB and intelligence products will focus on non-military information and civilian trends, as much as operational information.[10] In peace operations, the collection plans and IPB must also focus on non-military actors in the battlespace, such as NGOs, IOs, PVOs, police and para-military organizations, social, political, and religious organizations, and even commercial interests and enterprises providing important services. While IPB for a combat operation might have a unit or a location as a named area of interest (NAI), a peace operation NAI might be something more abstract like frequent meetings of local faction leaders, or observable events such as large movement of buses or transportation assets, or political rallies.

TFE-conducted IPB focused on FWF compliance with both the military and civil aspects of implementing the DPA. The focus of intelligence collection varied according to the situation. Intelligence relevant to the implementation of the military provisions focused on such issues as cantonment areas, weapons storage sites (WSS), displaced persons and refugees (DPRE), freedom of movement, and the right to inspect other sites. In supporting the elections, a civil operation for which the OSCE was responsible, TFE focused on monitoring cross-border refugee migration and voting corruption.[11]

Intelligence operations supporting a peace operation must be built with the premise that, historically, peace operations often prove to be long-term commitments.[12] As such, the RII obtained by various RISTA systems, HUMINT, open-source intelligence (OSINT), and ground reconnaissance and reporting were input into automated databases to support analysis and the development of predictive intelligence products over time.[13] TFE developed and maintained databases devoted to automobile license plates, key personalities, environmental issues, mass grave, imagery target deck, NAIs, and RFIs, without which, predictive analysis, mission management, and technical control would have been nearly impossible.[14]

Battlefield Visualization

Battlefield visualization is the process whereby the commander develops a clear understanding of his current state with relation to the enemy and environment, envisions a desired end state, and then visualizes the sequence of activities that will move his force from its current state to the end state.[15] From an IO perspective, the commander must first identify, then collect and process that critical information needed for battlefield visualization. In identifying the information required to support battlefield visualization, the commander must first establish his information requirements,[16] then continuously adapt these requirements based on METT-T. In collecting information, the commander must maximize the use of information acquisition means, dynamically tasking surveillance, reconnaissance and intelligence collection assets. Such a sequence of actions forms the friendly commander's information actions and has been referred to as shaping the "info-space."[17]

For the current state, he needs to know what is happening among the people who live in the operational area, key actors who can influence events in the AO, as well as friendly and adversary military force information. For the desired end state, he needs to collect information about both military and non-military actions that may occur once military objectives are secured. For visualizing the sequence of events leading up to the desired end state, he needs information to capitalize on friendly IO capabilities and take advantage of adversary IO vulnerabilities.[18]

Open-Source Intelligence (OSINT)

TFE refined its open-source collection to produce daily reports for commanders. One product called ***The Night Owl,*** provided RII on events in the area of operations, area of responsibility, and area of interest. The *Night* ***Owl,*** translated information from open-source media, primarily from the nations of the former Yugoslavia, providing insight into the concerns, politics, and psyche of the various FWFs. The MND-N Coalition Press Information Center (CPIC) produced the Daily Media Summary/Analysis which provided a quick summary and analysis of media stories from domestic and international sources. The Daily Civil Military Operations Center (CMOC) Report provided daily updates on CMOC projects as well as reports from the field on attitudes from the populace. SHAPE and SFOR News provided daily media summaries and analysis.

The PA component of TFE has captured RII on more than one occasion. In one instance during early operations in OJE, an international television reporter received information alleging the location of a mass grave site. He requested assistance from the JIB (precursor to the CPIC) and the information was passed to the G-2. In another case, the TFE Main CP had received word that there would be a protest at the front gate of Eagle Main (TFE's Main Base Camp near Tuzla). The JIB was able to call six local news media outlets (using translators) and the local ministry of internal affairs to confirm that no such protest was planned.[19]

Human Intelligence (HUMINT)

HUMINT is the most important discipline in many MOOTW activities for collecting information and understanding the AO. Whether collected by U.S., coalition, or host-nation personnel, HUMINT contributes the most to understanding the population, its culture, needs, and intentions, as well as the operational environment. HUMINT in MOOTW is often derived from non-MI military and civilian personnel in the AO. Workers from the IOs, PVOs, and NGOs operating in the battlespace are sources of information during MOOTW. In MOOTW, every individual is a potential source of HUMINT.[20]

The nature of peace operations is one of heavy involvement with the populace, governments, police, and military elements of the FWF, which makes intelligence collection HUMINT-intensive.[21] Human intelligence will often remain the only source of reliable information about the situation, even with today's highly technical battlespace, especially in MOOTW situations.[22] Operational concerns and internal security during MOOTW emphasize use of HUMINT.[23]

Capturing CCIR

Some information requirements may be filled by organizations which play a part in the Military Information Environment (MIE) in a theater of operations, but which do not communicate with the military communications architecture. The Military Information Environment (MIE) includes several actors operating outside the military information systems, such as UN offices, IOs, NGOs, PVOs and police. Occasionally, **"social and cultural elements, including religious movements and their leaders" or "adversaries and other non-DOD organizations including many actors, agencies, and influencers outside the traditional view of military conflict, intrude into the MIE...Their activities may cause an unanticipated or unintentional effect on military operations.**[24]

These "other actors" have become the focus of military operations during OJG. Accordingly, the CCIR in these operations focused on these groups which did not follow conventional military lines or actions. Task Force Eagle had to expand its abilities to acquire the RII it needed to plan and execute operations that would maintain situational dominance over these new actors. In peace operations, the most timely, accurate, or relevant information, may come from other than the traditional collectors of information through sources outside the unit or military channels.[25] Indeed, the information needs of the commander may be answered by the interface with local or international police, the news media, UN offices, Non-Governmental Organizations (NGOs) and Private Volunteer Organizations (PVOs), or private religious or social groups.[26]

The commander may need information that is shared in the communications infrastructure of these organizations, but is not routinely shared with the military component because of a lack of communications links, or deliberate efforts to conceal their actions and intentions. The commander may selectively task his Intelligence Surveillance and Reconnaissance (ISR) and Targeting and Acquisition assets to collect on, and may direct his staff to effect liaison with, the communications networks of these organizations to acquire the necessary RII and CCIR.

CCIR may be obtained by non-traditional intelligence collectors and from significant actors who intrude into the MIE. In TFE, the PMO, POLAD, interpreters, and SJA were each on various occasions the best means to collect the CCIR for the Division Commander. In each case, established liaison was exploited to extract the necessary CCIR in support of military operations.

In one case, a Federal Agency, the U.S. Information Agency (USIA) was conducting routine information-gathering efforts through a Bosnia-wide survey to support federal agencies involved in the diplomatic and economic aspects of the mission in Bosnia.[27] The Division PYSOP Support Element (DPSE) co-opted this effort to obtain necessary information to obtain a sharper focus on the target audience by gaining a better understanding of its perceptions on various issues. The USIA was glad to oblige and collected information in support of military operations in a less-intrusive manner than would have been the case if Tactical PSYOP Teams (TPTs) had been used.

Battlespace Awareness

The Department of Defense initiated support for Task Force Eagle under the C^4I for the Warrior Bosnia Command and Control Augmentation (BC^2A) program, which brought together a consortium of DoD components to meld communications and functional applications into an integrated whole with better connectivity, while taking advantage of the latest commercial technology.[28]

Task Force Eagle's situational awareness (SA) systems included its helicopter aviation assets, supporting Unmanned Aerial Vehicles (UAVs), JSTARS, RIVET JOINT, Airborne Reconnaissance Low (ARL), the USN Orion P-3C aircraft,[29] and other USAF and USN airborne-reconnaissance systems.[30] These assets were focused on COMEAGLE's CCIR (Commander's Critical Information Requirements) and on the potential and actual hot spots identified by the G-2. These systems were supplemented with HUMINT collectors, both active and passive. The aerial assets could be used *during* operations to provide battlefield visualization in support of current operations. The RISTA systems were carefully managed to ensure optimal use and were employed according to collection plans developed by the ACE on the previous day. Aviation provided a reconnaissance capability that could be rapidly redirected to focus on developing hot spots and provide reports and analysis. The shared RCP for the task force was communicated over the radio net.

Video cameras were an important tool in acquiring RII and documenting the facts when dealing with the FWFs and non-combatants. The saying "a picture is worth a thousand words" has meaning in IO directed at influencing FWF leaders and non-combatants. U.S. Army IO doctrine lists video-taping as a TTP for documenting actions and developing situations and states that **"...successful peacekeeping depends on impartial, factual reporting accompanied by as much pertinent data as possible: for example, photographs...[and] using video cameras and cassette recorders."**[31] In Operations JOINT ENDEAVOR and JOINT GUARD, even hand-held video "camcorders" at the squad and platoon levels were effective tools in acquiring RII and conducting C^2-Protect IO.

Imagery supported situation dominance over the FWFs during initial operations to separate the warring factions. Knowledge of the exact location and disposition of adversary heavy equipment via RISTA systems allowed friendly force commanders to pressure FWF military leaders into compliance, by demonstrating that friendly forces could see and target heavy weapons and vehicles in the battlespace. In these cases, the friendly commander could show the imagery to the FWF leadership – proof the FWF leaders could not refute – and direct them to move specific pieces of equipment, or risk their destruction.[32] **"Through IO, the Implementation Force (IFOR) always knew where the rival factions were and what they were doing. This enabled IFOR to control the situation on its own terms."**[33]

Capturing the CCIR by Exploiting Non-military INFOSYS

Some information requirements may be filled by international organizations that are part of the Military Information Environment (MIE) in a theater of operations, but which are not connected with the military communications architecture. The commander must be ready to exploit the communications processes and events between these organizations to meet his information requirements.

As previously explained, the most timely, accurate, or relevant information, particularly in MOOTW, may come from sources outside the unit or military channels. The MIE includes several actors operating outside the military information systems, such as UN offices, IOs, NGOs and PVOs, religious and social groups, local and international police, and the media. The commander may need information that is shared in the communications infrastructure of these organizations, but is not routinely shared with the military component because of a lack of communications links. The commander may selectively direct liaison between his staff and the communications networks of these organizations.

On 11 July 1997, the Association of the Women of Sebrenica attempted to execute a bus ride and vigil to the Dulici Dam, the suspected mass grave site of the victims of the genocidal slaughter of the citizens of Sebrenica captured and subsequently killed by Bosnian Serb Army in the Summer of 1995. As the AWS members and others began to board busses, an angry Bosnian Serb crowd gathered at the Dulici Dam to ambush the Bosniacs. Reports from the IPTF officers on the ground verified that the crowd was armed with pitchforks, rocks, and some small arms as well. At the final rehearsal on the night prior to the operation, the IPTF Regional Chief, a Russian Civilian Police Officer, briefed the compromise plan that had been reached, and the various contingencies that IPTF were prepared to handle. Additionally, he provided a sketch of the Dulici Dam area and explained the security concerns from the point of view of the IPTF. The IPTF representative was able to coordinate his plan with that of SFOR, and to fill information gaps SFOR had on the situation.

During the execution of the operation, the IPTF updated TFE on the situation developing at the dam site, and radioed through their chain of command and then to the MND-N CP through the Liaison Officer (LO). The Division TAC knew relatively quickly that an IPTF vehicle had been stoned and had an accurate description of the crowd growing at the dam site. This improved the division's situational awareness.

FM 100-6, *Information Operations,* lists "exchanges with local police" as a source of relevant information and intelligence.[34] The meeting arranged by the Tuzla Chief of Police with SFOR and the leadership of the AWS are real-world examples of this principle. Additionally, the coordination with the IPTF into the rehearsal and execution of the operation provided written and electronically transmitted Relevant Information and Intelligence (RII) that demonstrated the principle that RII "drawn from the MIE supports the creation of situational awareness and contributes directly to effective C^2 during all stages of the decision and execution cycle."[35] **The Division TAC was able to maintain an accurate Relevant Common Picture made more accurate by local police and IPTF input.**

Including the International Police Task Force in the planning and wargaming phase, and then maintaining communications in the execution phase helped TFE to maintain situational awareness during the Association of the Women of Sebrenica march on 11 July 1997. The Association of the Women of Sebrenica is an example of what **FM 100-6, *Information Operations,*** describes as **"Social and cultural elements, including religious movements and their leaders."**[36]

"The most timely, accurate, or relevant information, particularly in operations other than war (OOTW), may come from sources outside the unit or military channels."[37] **Indeed, "the information needs of the commander [may be answered by]...interface with local or international police...."**[38]

Battlespace Awareness – JCO as the Commander's "Directed Telescope"

The technique of the "directed telescope" employs the selective and careful use of trusted subordinates to serve as the commander's eyes and ears, to observe and report directly, rapidly circumventing command channels. Throughout history, commanders have used the "directed telescope" to obtain critical information requirements and to focus sharply on any part of the battlespace and rapidly acquire the information without filtering through layers of command hierarchy. The "directed telescope" is also a means for the commander to receive information on the "intangibles" such as friendly force morale, and attitudes, intentions, and perceptions of the local populace.[39] The "directed telescope" concept is usually accomplished by "using special operations units, reconnaissance teams or officers, and special communications networks."[40]

One of the most reliable sources of RII came from the Joint Commission Observer (JCO) teams composed of U.S. Army Special Forces and U.S. Navy SEALs. The JCO mission evolved from the experiences of the British Army supporting the UNPROFOR peacekeeping operation. When the UN force began operations in BiH, the infrastructure was so disorganized that there was no way for key political and military leaders and communicators of any factions to discuss problems with their adversaries. The initial mission of the JCO was to maintain communications between the UN peacekeeping force and the FWFs, and to be the link for the various faction leaders to communicate. British forces supporting UNPROFOR developed composite units (JCOs) that were capable of operating amidst the local population, with the mission to gain the ground truth and maintain liaison with FWFs.

When the Allied Rapid Reaction Corps (ARRC), later to be the Implementation Force (IFOR), assumed the mission, the JCOs were retained. The JCOs specifically communicated issues between the NATO commander and the political and military leaders of the FWFs. In that role, the JCOs were able to provide excellent RII on the intentions and actions of FWF leadership. Living among the local populace in "safe houses," the JCOs had a unique vantage point for collecting RII. The JCOs spoke the language, or used translators, and participated in cultural, social, and other local events, meeting daily with varied elements of the Bosnian society: FWF organizations, church authorities, local police, prominent citizens, refugees.[41] Through the Office of High Representative (OHR) and various faction liaisons, JCO operations monitored the pulse of the local populace. The JCOs observed potential flash points, such as refugee resettlement issues, political issues, and border disputes, which enabled commanders to be proactive rather than reactive.

The mission of the JCO in OJE/OJG/OJF was to assist FWF Leaders liaison with designated MND Commands in support of SFOR objectives and to be prepared to respond to a crisis by serving as a communications conduit between responsible elements to defuse or minimize the crisis. JCOs served as the division commanders' "directed telescope" regarding FWF activities, capabilities, attitudes and intentions. Being the "directed telescope" for the commander means being at the exact point on the battlefield which best answers the commander's information requirements. Their collocation among the local populace meant they were often the most credible source of information regarding the FWF.[42] As such, JCO represent a part of the friendly force INFOSYS in that the JCO personnel provide commanders with accurate, relevant, timely, and usable information that contributes to development of the relevant common picture and better situational awareness.[43] INFOSYS includes not only electronic and automated systems and equipment, but also the personnel who collect information that contributes to the knowledge of the battlespace.

The JCO METL includes:

- **Serve as impartial honest brokers**
- **Provide ground truth**
- **Assist FWF liaison**
- **Respond to crisis**
- **Coordinate with NGOs and Civilian Authorities**
- **Flatten the communications hierarchy**

Battlespace Awareness -Capturing and Distributing RII with Video

Video imagery has proven to be a powerful tool in Operations JOINT ENDEAVOR and JOINT GUARD. TFE was successful in countering propaganda and compelling compliance with the provisions of the DPA by demonstrating the means to capture non-compliance "on tape." Several systems were used to capture the facts, or information, that supported reporting, and situational awareness on the actions of the EAFs, para-military and police organizations, social groups, and non-combatants.

One of the simplest means of this technology was employed by soldiers on the ground during operations using hand-held video cameras. The ability of such simple systems to compel compliance and provide archival truth was demonstrated convincingly during Operation JOINT FORGE in the winter of 1998.

During a Weapons Storage Site (WSS) inspection in the American sector of SFOR in Operation JOINT FORGE, a company commander used a hand-held video camera to document potential non-compliance with the military terms of the General Framework on the Agreement for Peace (GFAP). Following the sensational arrest of Bosnian Serb General Radislav Krstic, a high-profile person indicted for war crimes (PIFWC) on December 2, 1998, the Bosnian Serb Army responded with non-cooperation with U.S. forces attempting to carry out Joint Military Commission (JMC) duties including inspecting WSSs. General Momir Talic of the Bosnian Serb Army (VRS) announced the suspension of "almost all aspects of cooperation between the RS Army and SFOR."[44]

To document anticipated non-compliance, the Company Commander brought along a hand-held video camera to record every step of the inspection. The Company Commander would either re-assert his rights to inspect the WSS, or he would have documented proof of non-compliance that could result in the imposition of a ban on all training or movement of the Entity Armed Forces (EAF).

Arriving at the WSS, the Americans found the EAF uncooperative, but the video camera, prominently forward with the Company Commander forced them to be accountable for their actions. The EAF complied with the Company Commanders demands, knowing that if they did not comply, they would be held accountable by SFOR. The EAF at the WSS repeatedly protested the need for the video camera, but their protests only served as a testimonial to its effectiveness in forcing compliance with the military provisions of the peace agreement.

Doctrine recognizes that **the use of video cameras contributes to "factual and impartial reporting (which) constitutes the cornerstone of all successful PKOs.**[45] Task Force Eagle distributed hand-held video cameras throughout American units in the Division to enable soldiers to document acts of non-compliance on the part of EAF and Entity police forces. During the Summer of 1997, when the task was dismantling illegal police check-points hindering freedom of movement, the hand-held cameras were identified as an important tool in documenting both non-compliance as well as documenting American actions to head off possible propaganda and disinformation from those opposed to SFOR actions.[46]

TTP: Hand-held video cameras give U.S. Forces a powerful tool with which to document non-compliance on the part of the military forces of the former warring factions (FWFs). This capability in and of itself is a way to compel compliance from FWFs military elements during tactical operations. Additionally, the video record serves as archived factual truth of the interaction between American forces and the FWF, and is available to refute adversary propaganda attacking the conduct of the peace operations force. Having recorded video imagery of the facts is an example of a C^2-Protect measure where the video itself may serve as the tool to counter "the effects of adversary propaganda or misinformation through PSYOP and PA."[47]

Battlespace Awareness JSTARS, UAV Aviation, and USN Orion P-3C can all provide Situational Awareness in Peace Enforcement operations.

TFE employed helicopter aviation and supporting JSTARS, UAV and P-3 assets during operations to track EAF units, police forces, political leaders, PIFWCs (Persons Indicted for War Crimes), organized groups of demonstrators, and unruly mobs. These assets were focused on COMEAGLE's CCIR (Commander's Critical Information Requirements) and on the potential and actual hotspots identified by the G-2. These systems were supplemented with HUMINT collectors, both active and passive. The aerial assets could be used during operations to provide battlefield visualization in support of current operations.

JSTARS The Joint Surveillance Target Attack Radar System (JSTARS), an IMINT collector, first deployed to support OJE on 14 December 1995. During ground operations on 13 January 1996, the U.S. bde of TFE employed a Ground Station Module (GSM) which received JSTARS information. Such use represented the first time a JSTARS GSM had been tasked down to a BDE in a real-world deployment. Initially, the GSM monitored large sectors, making analysis of specific areas difficult. As a result, the S2 narrowed the focus of the JSTARs by orienting the system on Named Areas of Interest (NAI) for specified periods of time. He also provided the operators, who also performed limited analysis, PIR and likely patterns to observe.[48]

However, it was discovered that JSTARS has certain limitations in a peace operations environment which preclude its employment as a "stand alone" collection asset. The non-linear, and for the most part, non-violent nature of peace operations means that civilian traffic may mix with FWF military movements, the FWF armed forces may sometimes use civilian vehicles, and even coalition vehicles may be intermingled with FWF and non-combatant vehicular traffic, making positive identification difficult. TFE found that it was indeed difficult to distinguish the significance of large convoys, which were detected by the Moving Target Indicator (MTI). Although the Synthetic Aperture Radar (SAR) was used to further refine images of vehicles within the convoy, definite confirmation of the types of vehicles could not be obtained to the degree of detail required. The SAR was used to identify some trenchlines within the zone of separation (ZOS), but identification of the positions requires close observation and analysis. The SAR imagery does not provide the degree of resolution required for easy recognition of a target.[49]

Although JSTARS exhibited these limitations, the brigade experienced several successes with the system. TFE identified large movements out of the town of Odzak. After the S2 was alerted of the movements, Civilian and Military Operations personnel were sent to that location to determine the reasons. The reason was the fact the Serbs did not want to live in Odzak after the area had been transferred to the HVO (Bosnian Croat Defense Forces). In addition, JSTARs confirmed a ferry site in the vicinity of Odzak. The site was designated as an NAI for a period of several days, and the MTI detected the movement across the river. JSTARS identified two-three tanks in an assembly area by a Fixed Target Indicator (FTI) and confirmed, to some degree, by a SAR photograph. JSTARS also identified a rail-loading operation of armored vehicles at a railhead near Odzak. JSTARS seems to have its greatest utility during the initial phases of peace enforcement operations which are characterized by open hostile opposing forces which must be separated and stood down.

UAVs TFE used UAVs, such as Predator and Pioneer, extensively for monitoring important areas of interest such as the Zone of Separation, EAF cantonment areas, gravesites, troop movements, para-military and police activities, and civil demonstrations.[50] On 29 June 1997, UAVs complemented ground reporting in monitoring FWF political leadership during a political crisis within one of the FWFs.

The Republika Serpska President, Madame Plavsic, had been detained by authorities at the airport in Belgrade, and then deported to Republika Serpska where she was subsequently met by elements of the RS Police upon her arrival there. A rift between the supporters of Mme. Plavsic in the northern portion of RS and the supporters of ousted ex-president and indicted war criminal Radovan Karadzic had widened and threatened to deteriorate rapidly with a change in government not an unlikely outcome. The MND-N commander was concerned that Mme. Plavsic's freedom of movement might have been restricted and controlled by rogue elements of the RS Police. Mme Plavsic was located at a hotel in Bijeljina by SFOR soldiers; a meeting was arranged with a senior field-grade SFOR officer. After the meeting, SFOR granted Mme. Plavsic's request for an RS military helicopter to fly her to her support base in the town of Banja Luka, where VRS Army III Corps MPs and an anti-terrorist unit would guarantee her safety. The request was granted out of concern that the RS President's safety among her own police forces was in question.

The motorcade's movement to the helipad and the subsequent flight to the Rupes Military Academy at Banja Luka were televised to the Main CP from beginning to end by the Predator UAV, allowing SFOR to track her every movement. Had any rogue RS Police attempted to interfere, SFOR would have known immediately: a visible demonstration of information dominance.

USN Orion P-3C and Army Aviation During an operation intended to prevent a clash of non-combatants from opposing FWFs on 11 July 1997, TFE used the USN Orion P-3C aircraft, helicopter aviation to track groups of demonstrators. The Association of the Women of Sebrinica (WOS) attempted to execute a bus ride and vigil to the Dulici Dam outside of Zvornik on the RS side of the Zone of Separation (ZOS) -- the location of a suspected mass grave site of the victims of the genocidal slaughter of the citizens of Sebrenica captured and subsequently killed by Bosnian Serb Army in the summer of 1995. The plan called for the group to cross the ZOS and hold a rally at the dam with busloads of WOS members and anyone else who decided to attend. The RS Police Chief of Zvornik had already announced that he would not provide security for the group. Local Bosnian Serbs in the vicinity of Dulici had fore knowledge of the planned bus ride, and crowds armed with rocks

and pitch forks began to form at the suspected mass grave site at the same time that the group was boarding transportation.

The MND-N Commander's intent was to prevent any open hostilities from erupting that would be detrimental to the peace process. Accordingly, SFOR forces in MND-N would take all possible measures to keep the two sides from coming into contact. The RISTA assets available in support of the operation were the P-3 and the helicopter aviation units: the Predator was on a mission outside of the division sector. For this mission, ground elements were postured and directed based on the aerial intelligence obtained by P-3 and the helicopter pilots. The Division forward command post, the Tactical Action Center (TAC), was able to accurately track the location of center of mass and front-line trace of the moving groups of demonstrators, give descriptions of their composition, disposition, and potential courses of action, thus providing a clear Relevant Common Picture (RCP) throughout the MND-N AOR.

AH-64 Gun Camera Video as an IO Tool TFE used Digitized footage from the Apache attack helicopter gun camera to enforce compliance among the FWF armed forces and document violations of the DPA. The photographs produced from the footage were declassified and occasionally handed over the FWF to compel them to comply with instructions to withdraw weapons or move forces. These photos were "date-stamped" and showed the exact location with grid reference and, of course, had the signature "cross hairs" of the gun system, providing an "unsubtle but highly effective means of compelling compliance."[51] Gun camera footage from aviation reconnaissance of the ZOS downlinked in real time to the freeze-frame-capable Mobile Intelligence Tactical Terminal (MITT) provided the friendly force irrefutable evidence to show the FWFs any acts of non-compliance.[52] By showing proof, the peace operations force demonstrated information dominance and avoided having to resort to lethal means to enforce compliance.

Other RISTA systems employed by TFE included Aerial Reconnaissance Low (ARL), Lofty View UAV, while SFOR employed NATO-level RISTA assets such as NATO E3S and US E-2Cs. ARL, a fixed-wing U.S. Army airframe packaged with COMINT and IMINT sensors, deployed in support OJE on 28 January 1996. This aircraft primarily provided images for TF Eagle requirements. In one mission, COMEAGLE demonstrated the presence of NATO intelligence by having the FWF leadership view themselves via live ARL video down-link to the Joint Military Commission (JMC) meeting they attended.[53] Lofty View, a short-range UAV, operated from Sepurine Air Base, Croatia, occasionally supported TFE by providing video images that were downlinked in real time to TFE headquarters.[54]

Daily, the G-2 develops plans for Predator, P-3, and helicopter aviation to obtain the Commander's CCIR and to cover potential hot-spots. Therefore, what was available on any given day was a function of the IPB analysis done the day before, and on what assets are available after higher headquarters RISTA needs are filled. During the AWS demonstration, for example, the MND-N Commander would have employed the Predator UAV extensively, but it was on an SFOR mission out of sector.

TFE primarily used the RISTA assets of P-3 and UAV as well organic and attached helicopter aviation assets to maintain situational awareness during operations. Both the UAV and P-3 provided real-time televised imagery that facilitated command and control. Helicopter aviation was always available, even when P-3 and Predator were out of the Division sector. The helicopter pilots were rapidly responsive intelligence collectors on developing situations who provided important SITREPs over FM radio communications. The combination of these systems enabled the Division to achieve Information Dominance over the FWF organizations or groups under scrutiny, resulting in TFE achieving situational dominance.

Using Modern INFOSYS to Build RII.

Exploiting Human Intelligence (HUMINT)

> ***"In noncombat operations, HUMINT, open sources, and other government agencies provide timely information to augment the unit's more traditional battle-focused intelligence collection effort."***
>
> **--FM 100-6, *Information Operations***

HUMINT is the category of intelligence derived from information collected and provided by human sources. During OJE/OJG/OJF, U.S. intelligence units employed a suite of technical intelligence-gathering means, reflecting U.S. strengths in such systems. Other partner nations, namely the British and French, fielded specialized capabilities in HUMINT in the Allied Military Intelligence Brigade, which complemented the U.S. technological means of collection.[55] This example of cooperation demonstrates the advantages that accrue from multi-national operations. **FM 100-8, *The Army in Multinational Operations,*** directs intelligence operations officers to carefully research and employ all available assets across the MNF.[56]

In peace operations, information gathered by patrols, observation posts, and roadblocks provides a substantial amount of information for MI analysts to evaluate.[57] While every soldier is an intelligence collector, specialized units maintain greater exposure to the local populace and governmental and military elements of the FWF, and are better positioned to gather HUMINT. The information gathered from traditional means is compared to HUMINT to support intelligence analysis. Joint Doctrine for peace operations notes **"the best sources of information may be CA and PSYOP personnel."**[58] In MND-N, the units best-suited to collect HUMINT in TFE were the Multi-Discipline Counter-Intelligence (MDCI) personnel organized into Force Protection Teams (FPTs). Although gathering information is not their primary task, several elements are well-positioned to provide information and intelligence, to include HUMINT, such as: Tactical PSYOP Teams (TPTs), Civil Affairs Direct Support Teams (DSTs), and the special forces Joint Commission Observers (JCOs).

In MND-N, the TPTs were actively engaged with the local populace through dissemination missions and coordinating with key communicators through the sector on a routine basis. The PSYOP soldiers actively debriefed the G-2 on pertinent information gleaned in their missions.[59] TPTs spent a great deal of time disseminating PSYOP print products to the local populace and were keenly positioned to provide relevant reporting on points of interest in the civilian communities of the battlespace.

"CA forces, if used correctly, can complement the intelligence collection process, especially HUMINT."[60] CA doctrine recognizes that the nature of CA operations which requires CA personnel to develop and maintain a close relationship with the civilian populace puts them in a favorable position to collect information.[61] CA operations are closely tied to the intelligence functions and operations associated with the overall tactical mission. CA personnel have an intricate and important intelligence role during both the intelligence cycle and the operational planning sequence. CA personnel support HUMINT through referrals to intelligence personnel for interpreters, and civilians with special skills. However, CA personnel must avoid appearing to be intelligence agents, or risk degradation of their primary mission.[62]

Task Force Eagle's Counter-Intelligence FPTs were composed of CI Agents, interrogators, and military or contracted civilian linguists. These teams were formed from the division MI Battalion and corps/theater MI Brigades. Their primary mission was to collect tactical HUMINT to satisfy the supported commander's primary intelligence requirements (PIRs). Through sustained collection efforts, the FPTs were able to substantially increase the volume of RII from HUMINT sources.[63] In the first year of OJE, tactical FPTs generated over 3,000 Force Protection Information Reports (FPIRs), a major percentage of the task force collection effort.[64]

Joint Commission Observer (JCO) teams composed of Army Special Forces and U.S. Navy SEALs were excellent sources of HUMINT. The JCOs supported SFOR objectives by performing liaison functions between SFOR and the EAFs. Deployed throughout the AO, and living in towns and villages among the local populace, the JCOs provided "ground truth" of EAF and FWF military and civilian attitudes, intentions, and actions. In emergencies, the JCOs served as a direct link between COMSFOR and the EAFs. The nature of the JCO mission brought the teams into contact with numerous political and social groups, local leaders, police, and military elements of the FWF. One TFE Military Intelligence Battalion Commander estimated that over 80 percent of all useful intelligence reporting resulted from FPT and JCO collection efforts.[65]

Exploiting Open-Source Intelligence (OSINT)

> ***"In noncombat operations, HUMINT, open sources, and other government agencies provide timely information to augment the unit's more traditional battle-focused intelligence collection effort."***
>
> **--FM 100-6,** ***Information Operations***

The MI Battalion document exploitation team played an integral role in Information Operations (IO) as the TFE OSINT Cell. The information it produced was especially important in a PKO and during municipal elections in which numerous political parties participated. The news media comprised important elements of the information environment during Operation JOINT GUARD (OJG). The international press covered SFOR operations, diplomatic and political events, and other newsworthy events extensively. Perhaps more importantly, local and regional media not only reported on events, but some also actively supported the agendas of the various political parties and presented their broadcasts accordingly. The local populace were avid consumers of these broadcasts and often responded to the messages presented. Therefore, it was critical for the TFE commander and staff to be aware of news broadcasts and to conduct information operations aimed at promoting the truth and countering misinformation. The OSINT Cell's operations proved to be an effective conduit for focused, analyzed reporting on the public media.

The OSINT Cell monitored TV and radio broadcasts and produced translated, edited transcripts. The cell published three products:

● **The *"Night Owl"* was a daily news digest of report summaries from broadcasts throughout the AOR.** It was an unclassified publication disseminated to military elements within TFE and to other military and non-government organizations (NGO) by request.

● **Intelligence briefs were special assessments of media broadcasts which focused on short-term trends or themes identified by OSINT analysts.** It was published three times a week and provided directly to the TFE G2.

● **The *"Nut Shell"* was a special assessment of media broadcasts which focused on specific long-term trends identified by OSINT analysts over several weeks or months.** The ***Nut Shell*** was published every three to four months, as required.

These products shared the same purpose and characteristics:

☞ **To provide an accurate depiction of open-source information available to the local populace.**

☞ **To assist commanders and staffs in anticipating the public response to various TFE operations.**

☞ **To help commanders and analysts gain an increased appreciation for the political, cultural and social environment as reflected by the media.**

☞ **To present information "as is" to the greatest degree possible to accurately depict public sentiment.** Transcripts were edited only to facilitate understanding and improved readability.

The OSINT Cell's reporting often provided indicators to the TFE staff of events that would require a tactical response by TFE forces. It also proved to be a valuable tool for use in the TFE Information Operations effort. FM 100-6 states that **"C^2 Protect includes countering an adversary's propaganda campaign to prevent it from affecting friendly operations, options, public opinion, and the morale of friendly troops."** The OSINT cell provided the supported command with both timely and historical records of messages presented to the local populace. Commanders and the TFE Information Operations Working Group (IOWG) used the cell's reporting to plan IO themes and to gauge their effectiveness after implementation.

Monitoring On page 57 is an excerpt from the list of the media sources the OSINT cell regularly monitored. The complete list included 28 news sources.

COORDINATING DRAFT
Peace Enforcement Information Operations

Monitoring The following is an excerpt from the list of the media sources the OSINT cell regularly monitored. The complete list included 28 news sources.

ASSOCIATED PRESS
http://wire.ap.org

BH RADIO, NEWS AT 0000
Bosnian radio station from Sarajevo.

BH TV, NEWS AT 0000
Bosnian television station from Sarajevo.

BLIC
Flash, Serbian national daily from Belgrade.

DNEVNI AVAZ
Daily Voice, Bosnian national daily from Sarajevo.

DNEVNI TELEGRAF
Daily Telegraph, Serbian national daily from Belgrade.

HINA, Republic of Croatia news service
http://www.hina.hr.

LJILJAN
The Lily, Bosnian national weekly from Sarajevo.

RADIO SOLI, NEWS AT 0000
Croatian radio station from Tuzla.

RADIO SVETI JOVAN, NEWS AT 0000
Radio St. John, Republic of Srpska radio station. Received from Brcko OSINT.

RADIO TUZLA, NEWS AT 0000
Bosnian radio station from Tuzla.

REUTERS
http://www.reuters.com.

SERB RADIO, NEWS AT 0000
Serb State Radio Station 93.5 from Pale.

SLOBODNA DALMACIJA
Free Dalmatia, Croatian national daily from Split.

SRNA, Republic of Srpska news agency
http://www.suc.org/news/srna.

The G2 focused the cell's monitoring, analysis and reporting functions by tasking the cell with standing reporting guidance as well as specific guidance to meet mission-oriented collection requirements. Below is an example of the standing reporting guidance. It provided the cell with specific events or locations of interest (similar to SIR) as well as specific indicators (similar to SOR).

The G2 adjusted his OSINT reporting guidance based upon guidance he received from the TFE Commander, the IOWG, and all-source analysts in the ACE. Representatives of the OSINT Cell also attended G2 shift change briefs and staff "huddles" to ensure that they were aware of emerging mission requirements. The OSINT cell disseminated its products in either paper or digitized form according to the users' requirements. The ***Night Owl*** was distributed in paper copies locally and in digitized copies via the internet to military and NGOs outside the

Endnotes, Chapter Four

[1] Headquarters, U.S. Army Training and Doctrine Command, ***Force XXI Operations,*** **TRADOC PAM 525-5** (Fort Monroe, VA: TRADOC), 1 August 1994, Chapter 3.
[2] Headquarters, Dept. of the Army, ***Information Operations,*** **Field Manual 100-6,** op. cit. p. 4-0.
[3] Ibid. p. 4-3.
[4] Ibid. p. 4-1.
[5] Office of the Chairman of the Joint Chiefs of Staff, **Joint Publication 3-07.3*, Joint Tactics, Techniques, and Procedures for Peacekeeping Operations,*** Washington, DC, 29 April 1994, p. V-6. See also Headquarters, Dept. of the Army, ***Military Operations in Low-Intensity Conflict,*** **Field Manual 100-20** (Washington, DC: USGPO), 5 December 1990, p. 4-6.
[6] HQDA, ***Military Operations in Low-Intensity Conflict,*** **Field Manual 100-20** (Washington, DC: USGPO), 5 December 1990 p. 4-7.
[7] Information provided here on the composition of the MI Task Force was originally published in Center for Army Lessons Learned, ***B/H CAAT V Initial Impressions Report – Task Force Eagle Transition*** (Unclassified, Distribution Limited, Fort Leavenworth, KS: CALL), May 1997, p. 11.
[8] The WARLORD is a U.S. intelligence processing system employed in TFE operations. WARLORDs were placed at all brigade-level headquarters of those participants in OJE/OJG/OJF. The information on the WARLORD system is divided into categories of SECRET, NOFORN, SECRET-Releasable to NATO, SECRET-Releasable to IFOR/SFOR. To ensure that no compromise of classified material occurred, a three-step process was employed, which ensured that non-U.S. personnel were not allowed access to the WARLORD workstation. For more information, see Center for Army Lessons Learned, ***Operation JOINT ENDEAVOR- Initial Impressions Report – Initial Operations*** (Fort Leavenworth, KS: CALL), May 1996, p. 66.
[9] Headquarters, Department of the Army, ***Intelligence and Electronic Warfare Operations,*** **Field Manual 34-1** (Washington, DC: USGPO), 27 September, 1994, p. 6-2.
[10] Headquarters, Dept. of the Army, ***Decisive Force: The Army in Theater Operations,*** op. cit., p. 8-15.
[11] Headquarters, USAREUR, ***Operation JOINT ENDEAVOR, USAREUR Headquarters After-Action Report,*** op. cit., p. 81.
[12] Headquarters, Dept. of the Army, ***Decisive Force: The Army in Theater Operations,*** **Field Manual 100-7,** op. cit., p. 8-5.
[13] Again, the term RISTA, rather than ISR, is employed here to emphasize the role of Target Acquisition systems in developing RII.
[14] Headquarters, USAREUR, ***Operation JOINT ENDEAVOR, USAREUR Headquarters After-Action Report,*** op. cit., p. 84.
[15] Headquarters, Dept. of the Army, ***Staff Organization and Operations,*** **Field Manual 101-5** (Washington, DC: USGPO), 31 May 1997, p. 1-3.
[16] The commander states his information requirements as priority intelligence requirements (PIRs) and friendly force information requirements (FFIRs). He also determines what information about the friendly force must be kept from the enemy, which are essential elements of friendly information (EEFIs). The commander's critical information requirements (CCIRs) are comprised of PIR, FFIR, and EEFI.
[17] Chairman of the Joint Chiefs of Staff, ***Operational and Academic Research Topics,*** 19 August 1997, downloaded from http://www.dtic.dla.mil:80/mil-ed/97jrt/index.html
[18] Headquarters, TRADOC, Information Operations Division, Brochure, ***Information Operations*** (Fort Monroe, VA: TRADOC), 22 January 1997, p. 11.
[19] Center for Army Lessons Learned, ***B/H CAAT2 Initial Impression Report – Operation JOINT ENDEAVOR – Continuing Operations*** (Unclassified, Distribution Limited, Fort Leavenworth, KS: CALL), September 1996, p. 67.
[20] Headquarters, Department of the Army, ***Intelligence and Electronic Warfare Operations,*** **Field Manual 34-1** (Washington, DC: USGPO), 27 September, 1994, p. 6-2.
[21] Headquarters, Department of the Army, ***Decisive Force: The Army in Theater Operations,*** **Field Manual 100-7,** op. cit., p. 8-5.

[22] Headquarters, Training and Doctrine Command, ***Concept for Information Operations,*** **TRADOC Pamphlet 525-69** (Fort Monroe, VA: TRADOC), 1 August 1995, p. 10.
[23] Headquarters, Dept. of the Army, ***Decisive Force: The Army in Theater Operations*****, Field Manual 100-7,** op. cit., p. 8-15.
[24] Headquarters, Dept. of the Army, ***The Army in Multinational Operations,*** **Field Manual 100-8,** op. cit., p. 1-3.
[25] Ibid. p. 2-10.
[26] Ibid.
[27] For a discussion on the role of the USIA in information operations, refer to Chapter Three, PSYOP, page 13.
[28] William S. Cohen, ***Annual Report to the President and the Congress*** (Washington, DC: USGPO), April 1997, p. 232.
[29] Larry K. Wentz, ed., ***Lessons from Bosnia: The IFOR Experience,*** Command and Control Research Program (National Defense University, Washington, DC: NDU Press), 1997, pp. 67-68.
[30] For a complete listing of other systems, see William B. Buchanan, ***U.S. European Command Support of Operation JOINT GUARD (21 December 1996 - 20 December 1997)*** (Unclassified, Distribution Limited, Alexandria, VA: Institute for Defense Analysis, IDA Paper P-3389), 1998, p. III-19.
[31] Headquarters, Dept. of the Army, ***Military Operations in Low-Intensity Conflict,*** **Field Manual 100-20,** op. cit., p. 4-6.
[32] Yu Lin Whitehead, Maj., U.S. Air Force, **"Information as a Weapon: Reality versus Promises,"** ***Airpower Journal,*** Vol. XI, No. 3, Fall 1997, p. 50.
[33] David L. Grange, Maj. Gen., U.S. Army, and Col. James A. Kelley, U.S. Army, **"Information Operations for the Ground Commander,** ***Military Review,*** March-April 1997, p. 9.
[34] Headquarters, Dept. of the Army, ***Information Operations,*** **Field Manual 100-6,** 27 August 1996, Washington, DC, p. 6-19.
[35] *Ibid, p. 4-1.*
[36] Ibid.
[37] Headquarters, Dept. of the Army, ***Information Operations,*** **Field Manual 100-6,** 27 August 1996, Washington, DC, p. 2-10.
[38] *Ibid.*
[39] Gary B. Griffin, Lt. Col., U.S. Army, ***The Directed Telescope: A Traditional Element of Effective Command,*** Combat Studies Institute, U.S. Army Command and General Staff College (Fort Leavenworth, KS: CGSC Press), July 1991, pp. 1, 5, and 8.
[40] Headquarters, Dept. of the Army, ***Information Operations,*** **Field Manual 100-6,** 27 August 1996 (Washington, DC; USGPO), p. 1-10.
[41] For a more detailed account, see William B. Buchanan, *U.S. European Command Support of Operation JOINT GUARD (21 December 1996 - 20 December 1997)* (Unclassified, Distribution Limited, Alexandria, VA: Institute for Defense Analysis, IDA Paper P-3389), 1998, pp. III-24 and III-25.
[42] Larry K. Wentz, ed., ***Lessons from Bosnia: The IFOR Experience,*** op. cit, p. 70.
[43] See Headquarters, Dept. of the Army, ***Information Operations,*** **Field Manual 100-6,** op. cit., p. 5-0.
[44] ***Slobodna Bosna (Free Bosnia),*** Bosnian national semi-monthly, 5-11 December 1998, Sarajevo, as translated in ***The Tuzla Night Owl,*** Task Force Eagle, G-2 OSINT, Vol 3, Issue 342, December 8, 1998, p. 5.
[45] Office of the Chairman of the Joint Chiefs of Staff, **Joint Publication 3-07.3,** ***Joint Tactics, Techniques, and Procedures for Peacekeeping Operations*** (Washington, DC: USGPO), 29 April 1994, p. V-6. See also, Headquarters, Dept. of the Army, ***Military Operations in Low-Intensity Conflict,*** **Field Manual 100-20** (Washington, DC: USGPO), 5 December 1990, p. 4-6.
[46] See CALLCOMS observation 10007-17500, " Video Cameras as information operations tools during peace enforcement operations." Published in ***B/H CAAT 9 Initial Impressions Report: Operation JOINT GUARD, Task Force Eagle Operations*** (Fort Leavenworth, KS: CALL, Unclassified, Distribution Limited), March 1998, p. A-55.
[47] Headquarters, Dept. of the Army, ***Information Operations,*** **Field Manual 100-6** (Washington, DC: USGPO), 27 August 1996, p. 3-9.
[48] See Center for Army Lessons Learned, CALLCOMS Observation 10011-59136 (Unclassified, Distribution Limited).

[49] Larry K. Wentz, ed., ***Lessons from Bosnia,*** Command and Control Research Program, National Defense University (Washington, DC: NDU Press), January 1998, pp. 100-102. See also CALLCOMS Observation 10011-59136, **"JSTARS Employment at Brigade Level,"** Center for Army Lessons Learned.
[50] Larry K. Wentz, *ed.*, ***IFOR C [4]ISR Experiences,*** a report prepared for the National Defense University, Command and Control Research Program, working draft, as of 15 January 1998, p. 46. Downloaded from the CCRP Website at http://www.dodccrp.org/bosnia.htm#REPORTS/BRIEFINGS
[51] This photograph digitization capability was the result of an investment in commercial software and off-the-shelf equipment costing less than $1,000. See Kenneth Allard, **"Information Operations in Bosnia: A Preliminary Assessment,"** ***Strategic Forum,*** Number 91, November 1996, Institute for National Strategic Studies, National Defense University, p. 5.
[52] Headquarters, USAREUR, ***Operation JOINT ENDEAVOR, USAREUR Headquarters After-Action Report,*** op. cit., p. 88.
[53] Ibid., p. 87.
[54] Headquarters, USAREUR, ***Operation JOINT ENDEAVOR, USAREUR Headquarters After-Action Report,*** op. cit., p. 87.
[55] Ibid., p. 77.
[56] Headquarters, Department of the Army, ***The Army in Multinational Operations,*** **Field Manual 100-8,** op. cit., p. 4-2.
[57] Headquarters, Department of the Army, ***Intelligence and Electronic Warfare Operations,*** **Field Manual 34-1,** op. cit., p. 6-2.
[58] Joint Warfighting Center, ***Joint Task Force Commander's Handbook for Peace Operations,*** Fort Monroe, VA, 28 February 1995, p. 30.
[59] Center for Army Lessons Learned, ***B/H CAAT IX, Initial Impressions Report*** (Unclassified, Distribution Limited, Fort Leavenworth, KS: CALL), March, 1998, p. A-124, CALLCOMS file number: 10003-79460.
[60] Headquarters, Dept. of the Army, ***Civil Affairs Operations,*** **Field Manual 41-10** (Unclassified, Distribution Limited), op. cit., p. 6-3.
[61] Ibid., p. 6-2.
[62] Ibid.
[63] Center for Army Lessons Learned, ***B/H CAAT Elections Initial Impressions Report*** (Unclassified, Distribution Limited, Fort Leavenworth, KS: CALL), March 1998, pp. A-98.
[64] Center for Army Lessons Learned, ***B/H CAAT V Initial Impressions Report – Task Force Eagle Transition*** (Unclassified, Distribution Limited, Fort Leavenworth, KS: CALL), May 1997, p. 14.
[65] Center for Army Lessons Learned, ***B/H CAAT Elections Initial Impressions Report*** (Unclassified, Distribution Limited, Fort Leavenworth, KS: CALL), March 1998, pp. A-132.
[66] Headquarters, USAREUR, ***Operation JOINT ENDEAVOR, USAREUR Headquarters After-Action Report,*** op. cit., p. 197.

Chapter Five
Information Systems (INFOSYS)

The joint definition of an information system (INFOSYS) includes the entire infrastructure, organization, and components that collect, process, store, transmit, display, and disseminate information.[1] The Army definition of INFOSYS includes personnel, machines, manual or automated procedures, and systems that allow collection, processing, dissemination, and display of information.[2] Regarding peace operations, what is important to note in both of the definitions provided above, is that INFOSYS does not consist only of ***automated* or *electronic*** systems, but can be also manual and "low-tech." An objective of IO is to shape the environment and influence decisions. In peace operations, no matter the technological or operational complexity any adversary or friendly INFOSYS may have, in the end it is people who analyze and make decisions on the data their INFOSYS provides; therefore, human action is at the heart of all INFOSYS.[3] The commander in peace operations should consider his entire staff as part of his INFOSYS.

Current IO doctrine recognizes that military forces may often use non-military INFOSYS in conducting operations, which is especially true in MOOTW where military forces work with other agencies and in multinational coalitions. A non-military INFOSYS consist of those elements not under the control of the military force.[4] Examples of such non-military INFOSYS include:

- **U.S. and host-nation Public Switch Networks (PSNs) and postal and telegraph systems;**
- **Digital and cellular telephone systems;**
- **Commercial communications satellite systems;**
- **Commercially developed software applications;**
- **Commercial, international news media;**
- **Electric power systems that support information networks;**
- **Commercial receivers that use precision, space-based navigation systems such as GPS.**
- **Public-accessed databases and bulletin boards (Internet).**

However, the concept of non-military INFOSYS as explained in FM 100-6 ignores several INFOSYS operating in a peace operations environment which require almost no technical means of support, and occur with predictable regularity. Examples of such INFOSYS are the forums, working groups, and regular meetings of FWF civil, police, and military leadership, meetings of political and social organizations among the local populace, and meetings of the IOs, PVOs, and NGOs operating in the AO. Military IO in support of diplomacy in peace operations requires both information and useful forums in which to present that information to be successful.[5] Joint doctrine recognizes that INFOSYS includes forums of discussion and other media of communications that support decisionmaking.[6] TFE has exploited these kinds of INFOSYS to answer its information requirements and to disseminate elements of the IO campaign to decisionmakers and other actors whose operations intrude into the military information environment.

These organizations operate in the same battlespace, but with a different focus, and with different governmental, political, social, and military interface with the FWFs. **The routine meetings between the IOs, NGOs, PVOs and their FWF counterpart organizations and FWF governmental, political, social and military leaders represent a *"low-tech"* INFOSYS which influences FWF decisionmaking.** Civilian agencies operating in the battlespace "had developed a network of influential contacts, compiled historical and specialty archives, and established relationships with local leaders and businessmen. They understood the infrastructure of the region, and the political and economic influences."[7]

The commander may need information that is shared in the INFOSYS of the participating parties to such forums, but is not routinely shared with the military peace operations force due to either a lack of communications links or reporting procedures. Military interaction with civilian organizations in peace operations is more than civil-military cooperation. By tapping into the INFOSYS represented in these routine meetings, U.S. Forces enhance their information dominance. Because such meetings and forums are predictable, the commander can direct his staff to send appropriate personnel, either to directly participate,[8] representing the peace operations force, or get updates from the IO, NGO, or PVO representatives or their liaisons to the military force.

Other forums which constitute **"low-tech" INFOSYS** may be established by the peace operations force. Examples of INFOSYS either established or controlled by the peace operation force include the Joint Military Commissions (JMC), meetings of the Political Advisor (POLAD) with civilian leaders, and forums created by the SFOR or TFE in the battlespace which include the FWF civilian, police, or military leadership.

The Joint Military Commission (JMC) liaison offices established between SFOR and the Entity Armed Forces (EAFs) are at once: 1) a conduit of information for COMSFOR and his multinational division commanders to the military leadership of the EAFs; 2) a direct source of RII from EAF command and control echelons, and; 3) a venue to conduct IO aimed at influencing this important group of significant actors. The Political Advisor (POLAD) assigned to Task Force Eagle in the conduct of meetings with significant actors outside the military environment, but acting inside the MIE accomplished the same results of being both a source of RII and a venue for IO. The TFE POLAD's meetings with leaders of social, political, and religious groups, as well as civil leadership, enabled COMEAGLE to influence these important decisionmakers, whose actions can intrude into the MIE.[9]

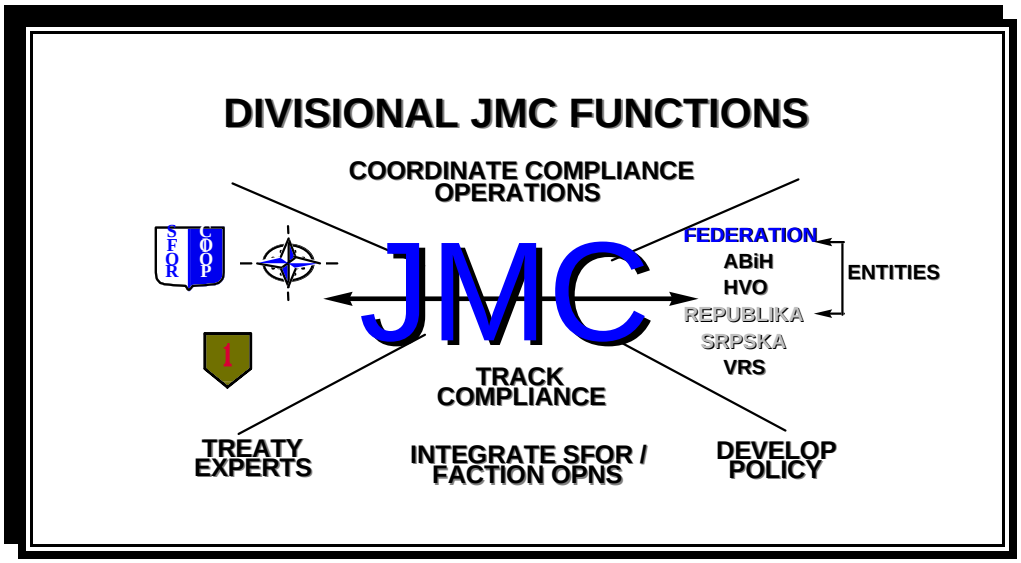
The weekly meetings between the Tuzla Chief of Police, the International Police Task Force, the Russian Brigade Military Police, and the TFE Provost Marshal provide yet another example of a low-tech INFOSYS comprised of people representing various organizations within an established forum that met regularly. The IPTF was also represented by an LO at the TFE Main Command Post when required. Daily reports from the 1,600-man IPTF covered issues important to TFE such as freedom of movement and human rights violations, demonstrations and rallies, crime, traffic safety, and inter-entity police cooperation. On more than one occasion, access to this INFOSYS answered COMEAGLE's CCIR for operations either planned or underway.

Although INFOSYS need not be technical in nature, U.S. Forces in Operation JOINT GUARD employed automated INFOSYS to aid in predictive intelligence analysis, controlling operations, and battletracking. TFE developed and maintained databases on environmental issues, mass graves, PIFWCs, key actors, vehicle license plates, police checkpoints, weapon storage sites, and target information.[10] As demonstrated in Chapter Four, TFE employed a sophisticated array of technologically advanced RISTA systems, which were an important part of the friendly INFOSYS that friendly forces both protected and exploited. While the communications infrastructure that supported TFE in Bosnia is without dispute an integral component of the friendly INFOSYS, its composition is largely a matter of technological capabilities of fielded systems and their tactical distribution and will not be discussed here. Chapter Five of FM 100-6 discusses at length the technical components of the present and future Army Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C^4ISR) systems.

Exploiting "Low-Tech" INFOSYS – The JMC

The Joint Military Commissions (JMC) established between SFOR and the Entity Armed Forces (EAFs) are a low-tech INFOSYS. The United Nations Security Council Resolution (UNSCR) 1031, which authorized member states to establish an Implementation Force (IFOR), under NATO control, also defined the FWFs' military responsibilities, IFOR's mandate rights and roles, and formally created the JMC. The JMC was chartered as a forum for military authorities to coordinate implementation of the military aspects of the GFAP.

The primary purposes for conducting JMC meetings during OJE/OJG/OJF was to allow COMEAGLE to track EAF compliance with the peace accord; to disseminate intent and instructions, and to coordinate activities or resolve differences between SFOR and the EAFs and between two or more of the EAFs. During OJG, COMEAGLE designated the JMC as the sole agency responsible for communicating and coordinating directly with Corps-level commanders and representatives, from the armed forces of the two entities, on implementation of all military aspects of the GFAP. Within MND(N), subordinate-level joint military commissions executed missions similar to those of the division task force, but at their respective levels.



The mission of the JMC at division level and below was to monitor compliance to provide information to the commander on the activities of the EAFs. These JMCs also allowed for disseminating policy, issuing instructions to factions on policies and procedures, coordinating the General Framework Agreement for Peace required actions, resolving military complaints, questions and problems, coordinating civil/military actions where appropriate, and developing confidence-building measures between parties.

The nature of peace operations is such that many events are known in advance; for example, Weapons Storage Site inspections, elections, DPRE resettlements, demonstrations and rallies, EAF training events, etc. In TFE, JMCs coordinated with the FWFs prior to a scheduled event. In addition, guidance was provided in fragmentary orders directing brigades and below to conduct JMCs and bilateral meetings with the FWFs. Division-level JMCs and bilateral meetings were conducted and letters, outlining Task Force Eagle's intentions and expectations, signed by the Division Commander, were sent to corps-level commanders of the FWFs. Finally, during the last few days before the event, joint commission officers ensured communications were established between the Division Headquarters and the headquarters of the FWFs.[11]

JMC operations and decisions required appropriate media coverage and were, therefore, coordinated with the PAO. Media coverage of JMC operations should be developed as a theme in the popular support campaign to emphasize the legitimacy and authority of the JMC. The aims are to reinforce the binding nature of JMC decisions, obligate local groups and individuals to comply, and underscore the consequences of noncompliance. Commanders can also improve the effectiveness of JMCs by recognizing the motivating power of self-interest among the local JMC participants. The key is to ensure that local JMC members have strong incentives for continuing to work through the JMC process. In addition, all sides must understand the penalties of obstructing or withdrawing from JMC operations. By doing so, commanders establish a pragmatic basis for influencing the behavior of local leaders and the groups they represent.[12]

In MND-N, the JMC process represented a low-tech INFOSYS, which enabled TFE to communicate to the FWF military leadership clearly. The JMCs gathered and maintained information on the preferences, positions, and understandings of the parties regarding the peace agreement, in fact, these were the JMC's CCIR.[13] These JMC meetings, at all echelons, provided the TFE Commander and his staff greater SA on the attitudes, intentions, and actions of the EAFs. The information obtained from these meetings often confirmed or denied reports from other sources and ensured that COMEAGLE maintained information dominance.

UN/NGO and Peace Operations Force Interface -- an Exploitable INFOSYS

Some information requirements may be filled by international organizations that are part of the Military Information Environment (MIE) in a theater of operations, but which are not interconnected with the military communications architecture. The commander must be ready to exploit the communications processes and events between these organizations to meet his information requirements.

As stated in Chapter Four, the most timely, accurate, or relevant information in military operations other than war (MOOTW), may come from non-traditional collectors and from sources outside the unit or military channels.[14] The Military Information Environment (MIE) includes several actors operating outside the military information systems, such as UN offices, Non-Governmental organizations (NGOs) and Private Volunteer Organizations (PVOs). The commander may need information that is shared in the communications infrastructure of these organizations, but is not routinely shared with the military component because of a lack of communications links. The commander may selectively direct liaison between his staff and the communications networks of these organizations.

An example of the conditions described above occurred in MND-N during Operation JOINT GUARD. After the opening of the Brcko bridge, both Croatian and Republika Serpska (RS) authorities imposed fees to cross the bridge in violation of the Status of Forces Agreements (SOFA) that are part of the General Framework on the Agreement for Peace (GFAP, a.k.a. the Dayton Peace Accord). In relation to the activities of the RS in this area, such action also violated the Constitution of Bosnia and Herzegovina. The TFE CG wanted to know more about the activity of the Croatian and RS customs authorities and the RS Border Police as well as their intentions, and directed the Division Staff to meet with the international offices in Brcko to assess the situation.

Because SFOR had already established liaison with the Office of the High Representative of the UN at Brcko, the TFE staff was able to take advantage of non-military information channels. The appropriate subject-matter experts for the issue were the Law Enforcement and Military Law elements of the TFE Staff. The Deputy PMO and DIV JAG convoyed to Brcko to attend a weekly meeting at the Office of the High Representative of the UN in Brcko whose regular attendees were the following:

- **OHR Representative**
- **SFOR LO to the OHR at Brcko**
- **European Union Customs Official**
- **IPTF Representative**
- **Civil Affairs Officer supporting the SFOR Liaison Office to the OHR**

At this meeting, the lead agents for SFOR, that is, the MP and JAG staff officers, were able to ask the right questions to fulfill the commanders information requirements for subsequent action. This event is an example of a situation where the necessary relevant information originates from a source outside the military communications channels, but is still a component of the Military Information Environment.[15]

Effective liaison with NGOs, PVOs, and International Organizations in the Area of Operations allows the commander to readily take advantage of information sources outside the military communications and information infrastructure, but still within the Military Information Environment. By maintaining awareness of the operations of these organizations, the commander may tap into their information systems, meeting, etc., employing the appropriate subject-matter expertise of the staff to fulfill his information requirements.

Establishing a Low-Tech INFOSYS in the Battlespace.

Peace operations forces may also create such forums within the battlespace that will serve to communicate information campaign themes to targeted audiences and influence FWF and social/political group leadership. An example of such a forum created by TFE is the Media Working Group. The MND-N and OHR-N sponsored a Media Working Group for the media representatives of the FWFs, which provided SFOR an additional information operations platform. IO require closer attention to the media and their intended and unintended effects on operations.[16] As stated earlier, the media in Bosnia was largely politically controlled, and reporting was biased by either omission of the truth, distortion through emphasis on only those elements of information which reinforced a political view, or outright disinformation, i.e., fiction-based propaganda. A Brigade PSYOP Support Element (BPSE) operating in MND-N arranged to form a standing Media Working Group of local media representatives. The location of the meetings had rotated between the BiH and R/S sides of the IEBL at neutral facilities. Attendees typically included the BPSE Commander, a PAO representative from the Coalition Press and Information Center, and 19 representatives from nine radio stations, with each of the FWFs being represented. The intent of the Media Working Group was to provide a forum where the media representatives of the FWFs could assemble to:

➜ Work on joint projects that would allow each faction access to news contacts and sources on the other side of the ZOS;

➜ Receive professional development through presentations and workshops;

➜ Obtain access to representatives from media representatives of other FWFs;

➜ Obtain access to the professional services and capabilities of the OHR public affairs section;

➜ Obtain increased access to SFOR information operations entities such as the CPIC (Coalition Press and Information Center) and the PSYOP BPSE and DPSE.

Task Force Eagle offered incentives to the FWF media representatives to gain their cooperation. These incentives took the form of increased access to unbiased information from the outside world via satellite downlink through SFOR offices in Sarajevo, technical assistance from experts working at the OHR PAO section, and access to information from the other FWFs in a safe environment. By creating the forum, TFE and SFOR obtained an additional platform for information operations over which it exerted considerable influence and to which it had unfettered access to all three FWF media groups. This forum presented an opportunity to expand access to local media and to improve both relations between SFOR and the FWF media and between the media representatives of the FWF.

Endnotes, Chapter Five

[1] Office of the Chairman of the Joint Chiefs of Staff, ***Command and Control Warfare,*** **Joint Pub 3-13.1,** op. cit., p. I-1.
[2] Headquarters, Dept. of the Army, ***Information Operations,*** **Field Manual 100-6,** op. cit., p. 5-0.
[3] Brian E. Fredericks, Col., USA, **"Information Warfare at the Crossroads,"** ***Joint Forces Quarterly,*** Summer 1997, No. 16, pp. 97-103.
[4] Headquarters, Dept. of the Army, ***Information Operations,*** **Field Manual 100-6,** op. cit., p. 5-5.
[5] Department of Joint and Multinational Operations, U.S. Army Command and General Staff College, ***The Nation and Military Power,*** Student Text S511, Lesson 1 (Fort Leavenworth, KS: CGSC Press), 27 March 1995, p. LSN 1-2-3.
[6] Office of the Chairman of the Joint Chiefs of Staff, ***Command and Control Warfare,*** **Joint Pub 3-13.1,** (Washington, DC, USGPO), 7 February 1996, p. v.
[7] Headquarters, USAREUR, ***Operation JOINT ENDEAVOR, USAREUR Headquarters After-Action Report,*** op. cit., pp. 88-89. See also, Larry K. Wentz, ed., ***Lessons from Bosnia: The IFOR Experience,*** Command and Control Research Program, National Defense University (Washington, DC: NDU Press), 1998, p. 61.
[8] Stephen W. Shanahan, Lt. Col., U.S. Army (Ret), and Garry Beavers, Lt. Col., U.S. Army, **"Information Operations in Bosnia,"** ***Military Review,*** Vol. LXXVII, No. 6, November-December 1997, p. 58. The authors mention TFE participation in International Housing Committee meetings as an example.
[9] Ibid. The authors describe both the JMC and POLAD meetings as IO "mediums."
[10] Headquarters, USAREUR, ***Operation JOINT ENDEAVOR, USAREUR Headquarters After-Action Report,*** op. cit., p. 84. See also Larry K. Wentz, ed., ***Lessons from Bosnia: The IFOR Experience,*** Command and Control Research Program, National Defense University (Washington, DC: NDU Press), 1998, p. 61.
[11] Fred Johnson, Maj., U.S. Army, Center for Army Lessons Learned, ***Tactics, Techniques, and Procedures for Civil Disturbance,*** **Newsletter No. 96-11,** November 1996, p. 20.
[12] Center for Army Lessons Learned, ***Joint Military Commissions,*** **Newsletter No. 96-8,** September 1996, p. III-10.
[13] Ibid, p. II-2.
[14] ***Information Operations,*** **Field Manual 100-6,** Headquarters, Dept of the Army, Washington, DC, 27 August 1996, pp. 2-6 and 2-10.
[15] Center for Army Lessons Learned, ***B/H CAAT IX, Initial Impressions Report*** (Unclassified, Distribution Limited), op. cit., pp. A-74 & A-75.
[16] ***Information Operations,*** **Field Manual 100-6,** Headquarters, Dept. of the Army, Washington, DC, 27 August 1996, p. 1-13.

Chapter Six
IO Staff Organization, Actions, Processes, and Products

Field Manual 100-6, *Information Operations,* addresses the formation and organization of a division IO cell, the structure of which is the prerogative of the commander. **"It may be something as simple as the periodic use of an expanded targeting cell or a more formal approach establishing a standing cell with a specifically designated membership."**[1] A Commander of Task Force Eagle suggested that for corps, divisions, and task force-sized units, "ad hoc" approaches to building the IO Cell might be the answer.[2] During OJG, Task Force Eagle's division's IO cell was comprised of the Division's IO officer and a three-man Field Support Team (FST) from the Land Information Warfare Activity (LIWA). A LIWA FST provides expertise in deception, OPSEC, and tools for IO modeling, targeting, and synchronization.[3] The National Ground Intelligence Center, in conjunction with LIWA, can support commands with specialized IO products.[4]

To fully integrate and synchronize all components of IO, TFE employed an Information Operations Working Group (IOWG). The weekly IOWG served the planning and wargaming and control functions of an IO Cell. Such a group is appropriate to peace enforcement operations where the optempo is somewhat more predictable than in combat operations. If the peace operation situation should move to open conflict, FM 100-6 states that it may be more appropriate to stand up an Information Operations Battle Staff (IOBS), to integrate information operations in the staff. **"The [IO] battle staff would consist of all staff members with a functional responsibility within IO, such as signal, fire support, PA, CA, OPSEC, EW, PSYOP, and military deception."**[5]

AR 520-20, *Information Warfare/Command and Control Warfare Policy,* established LIWA to support and integrate IO in Army operations. TFE's LIWA Field Support Team was the backbone of the IO Cell in MND-N. The working group was chaired by the LIWA FST Commander and was composed of representatives from the staff sections with a role to play in information operations, which included the following:

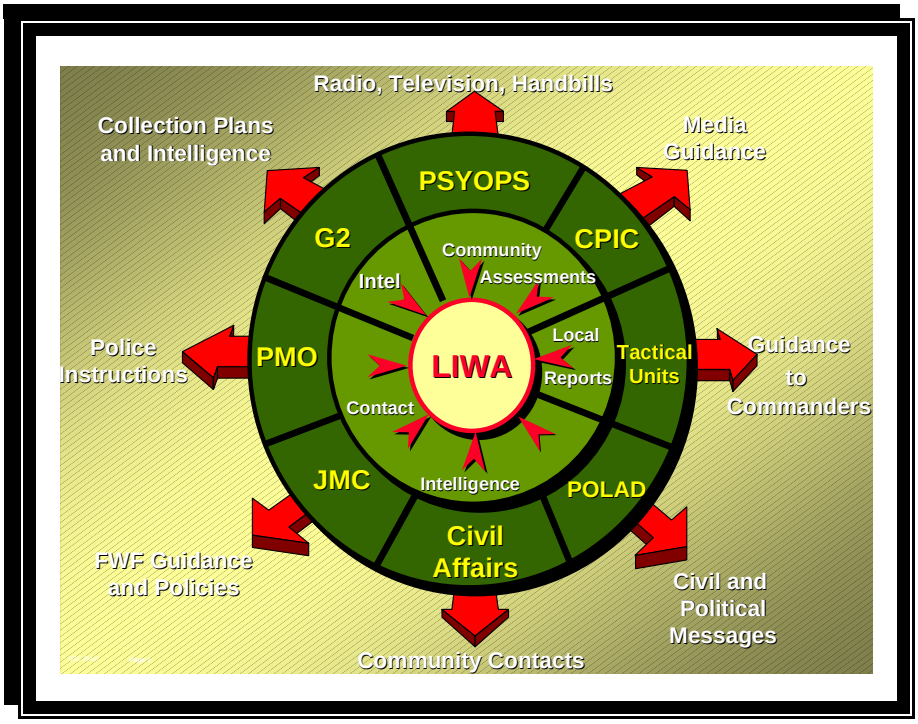
- **Division Public Affairs Officer**
- **Coalition Press Information Center Director (a senior PAO officer)**
- **Provost Marshal**
- **SOCCE (representing the JCOs)**
- **Staff Judge Advocate**
- **G-5 Civil Affairs**
- **G-2 Plans**
- **G-3 Plans**
- **Allied Brigade Liaison Officers**
- **Task Force Liaison Officers Joint Military Commission Representative**
- **PSYOP, DPSE Commander**
- **Political Advisor (POLAD)**

The functions the IOWG performed included:

- **Planning the overall IO effort for the commander;**
- **Developing IO concepts to support the scheme of maneuver;**
- **Establishing IO priorities to accomplish planned objectives;**
- **Determining the availability of IO resources to carry out plans.**[6]

In TFE, the IOWG coordinated and synchronized the actions of the IO actors in the operations planning phase by brainstorming how each actor could contribute to a coordinated IO Campaign that would support the Commander's intent and achieve the desired end state. The IOWG would organize these actions into a synchronization matrix built on IO Campaign Themes developed by the LIWA FST. To support operations, the IOWG developed a draft Information Operations Mission Statement and commander's intent for IOs in support of specific CONPLANs and operations, and in support of the overall peace enforcement mission. For all operations, the IOWG developed IO themes to communicate to the target audience(s) to achieve the desired endstate. In peace operations, IO themes must "concentrate on proactive versus reactive efforts to: reduce sources of conflict; assist nations in the transition to democracy; increase international dialogue and understanding; build political, economic, military, medical, commercial, social, and educational bridges; emphasize the role of the military in a democracy; and highlight the constructive domestic uses of the military."[7]

IO Themes were incorporated throughout the various elements of C^2W, CA and PA. PSYOP integrated the IO Campaign themes into PSYOP radio, television, and print products (posters, handbills, etc.). PA integrated the themes into press releases at Coalition Press Information Center press conferences, and in articles appearing in command information publications. Civil Affairs DSTs reinforced the themes when supervising civil-military projects and when conducting liaison with local officials. Commanders from Battalion Task Force level to SFOR were interviewed on local radio shows. PSYOP-sponsored media working groups reinforced the IO Campaign themes. The TFE PMO reinforced the IO Campaign Themes in his interaction with the International Police Task Force (IPTF) and local police. The POLAD did the same in all interaction with IO/NGO and local leaders. And, finally, the Joint Military Commissions did the same in their interaction with the EAFs. In addition, the IOWG would produce the IO component of all CONPLANs and FRAGOs issued to the Task Force. In short, the IOWG served as the hub for all IO as portrayed in the following diagram.



The IOWG was most effective in planning and wargaming for IO in support of actual operations, when time was not a constraint. In Peace Operations designed to return the FWFs to normalcy, events along the way, such as elections, resettlements, and weapons storage site inspections, for example, are planned well in advance. Other actors in the Global Information Environment, such as religious or political groups, may also plan their own events, which intrude into the Military Information Environment and affect military operations. Extremists may demonstrate, counter-demonstrate, boycott, or sabotage these events to derail the peace process. For these kinds of events that are known in advance, the IOWG had time to develop a comprehensive IO component to the Operations Order (OPORDER) that supported successful execution of the military operations aimed at maintaining situational dominance - controlling the events and actors of the battlespace.

Information Operations require detailed planning and longer lead time for execution. This is necessary to ensure all components of the IO Campaign are functioning during the "preparation of the objective" phase with non-lethal fires from the IO actors to create the conditions for successful accomplishment of the operation and achieving the commander's desired end-state.

In Peace Operations designed to return the FWFs to normalcy, events along the way, such as elections, resettlements, and weapons storage site inspections, for example, are planned well in advance. Other actors in the Global Information Environment, such as religious or political groups, may also plan their own events, which intrude into the Military Information Environment and affect military operations. Extremists may demonstrate, counter-demonstrate, boycott, or sabotage these events to derail the peace process. For events that are known in advance, the IOWG had time to develop a comprehensive IO Campaign that supported successful execution of these types of operations. These known events are examples of ***Problem Sets.*** A Problem Set is defined as "a group of related issues or events that, in the opinion of the commander, could significantly hamper or jeopardize mission success."[8] Examples of such problem sets include:

- **Territorial disputes;**
- **Resettlement operations;**
- **Law and order;**
- **Refugees and Displaced Persons; and,**
- **Force Protection**

Problem sets encountered in Bosnia by TFE included the municipal elections scheduled for September 1997, and the planned march of the Association of the Women of Sebrenica (WOS) to the Dulici Dam in Republika Serpska on 11 July 1997. For the municipal elections, themes were developed to support each phase of the preparation, execution, verification and implementation of the voting process and its results. These themes were incorporated into products and actions to be produced and disseminated by the IO actors in the division (CA, PSYOP, JMC, SJA, POLAD, PAO, and the Joint Information Bureau (CPIC)). The themes were developed by phases to ensure that the messages and products were precisely focused to modify behavior to achieve the desired outcome.

For the WOS march, the division developed a FRAGO for the operation and wargamed its execution to develop the branches and sequels to the basic plan. The purpose of the operation was to keep two groups of protesters separated to prevent an outbreak of violence and maintain the peace. For this operation, the themes stressed leading up to the march were "Freedom of Movement" and "SFOR has the means and resolve to enforce the Dayton Peace Accords and that individuals or groups should not provoke violent actions." These themes were intended to influence the behavior of both groups, to convince the Bosniacs (Bosnian Muslims) not to provoke a response by demonstrating on the RS side of the IEBL, and to convince the Bosnian Serbs not to interfere with freedom of movement.

Task Force Eagle's Information Operations Process

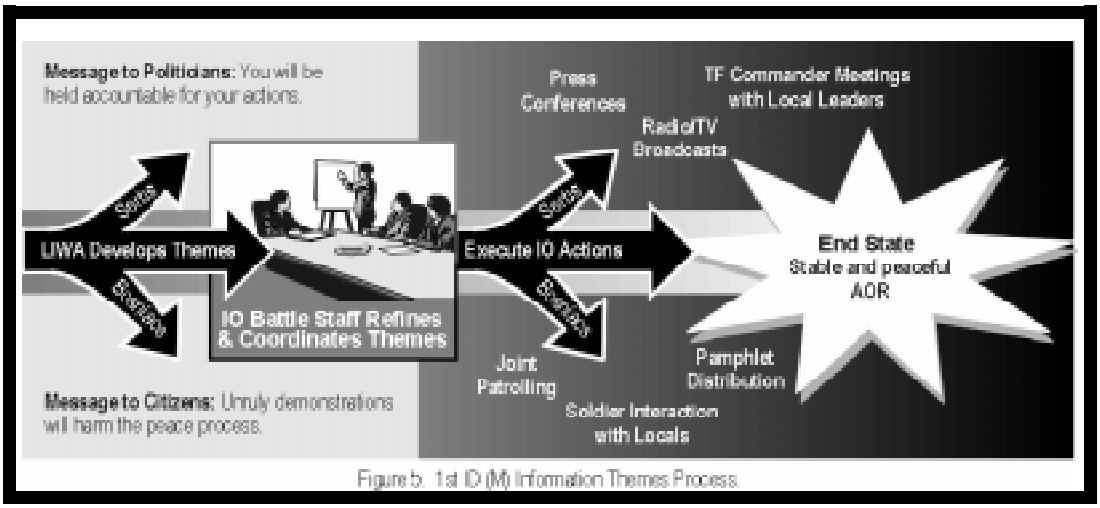


Figure b. 1st ID (M) Information Themes Process

The IO planning process employed in Operation JOINT GUARD (OJG) was very effective for missions of long lead-time and resulted in a coordinated IO component to Division CONPLANs. The IO Cell in OJG was the Information Operations Working Group (IOWG) which, through a series of meetings, would brainstorm, wargame, coordinate, and synchronize the actions of the various staff sections contributing to IO courses of action in support of developing CONPLANs. The planning cycle for TFE IO began with the Wednesday meeting of the IOWG, where the FST Cdr guided the discussion about IO activities within the working group. From this meeting, the LIWA FST Cdr built the IO FRAGO. The next phase of the cycle occurred the following day when the FRAGO (fragmentary order) for IO was issued, directing the appropriate staff elements or units to conduct IO for the following two-week period. Included in the FRAGO was a report format specific to IO terminology and issues. The final phase of the cycle ended on the following Monday, when units and staff elements reported their IO input to the LIWA FST Cdr. Units and staff elements assigned IO tasks had five days to execute and then report, allowing the LIWA FST Cdr two days to incorporate the reports into the next FRAGO.[9]

IO Staff as the Division Main Effort in the Main CP

The Division Main CP, established by the first U.S. Division in the Bosnian theater, and subsequently passed on to following divisions at Eagle Base, Tuzla, was specifically arranged and designed to support Peace Enforcement operations vice mobile combat operations. The Main CP was arranged with those battlefield functional areas contributing to information operations being the ***Main Effort.***

It is the nature of peace enforcement operations to transition from combat operations to stability and support operations aimed at establishing normalcy to the area of operations, that is, to return the area to a state of peace. As conditions return to normal, the combat arms emphasis so necessary in the initial entry phase of the operation for separating the belligerents, gives way to an emphasis on those battlefield functional areas which support the efforts of the FWFs in implementing the agreement, and will help the country to rebuild. These functional areas are Civil Affairs (CA), Psychological Operations (PSYOP), Public Affairs (PAO), Staff Judge Advocate (SJA), the Joint Military Commission (JMC), Provost Marshall (PMO) and the International Police Task Force (IPTF), the Land Information Warfare Activity FST Commander, and the Special Forces Joint Commission Observers (JCOs).

The arrangement of the Multi-National Division-North Main CP reflects that the staff cells of these battlefield functional areas were indeed the main effort of the division's operations, as they were in the front row facing the Commanding General and his immediate staff. In laying out the Main CP, the 1st Armored Division emphasized these staff cells and individuals **"after two months of wargaming confirmed that the most likely actions would involve non-lethal means, backed by an appropriate military support to encourage compliance...direct military action was to be avoided to create an atmosphere of friendly cooperation."**[10] The increased importance of these special staffs, and the need to include them in operations, led the 1st Armored Division to construct larger C^2 facilities to accommodate them into the CP architecture.[11]

Information Operations were often the Main Effort for Operations JOINT GUARD and JOINT FORGE. That the layout of the Main CP should reflect this makes sense and clearly demonstrates their contribution to mission accomplishment. The logical physical arrangement of the cells and staff sections supporting information operations supported interaction between them, resulting in greater synchronization of effort in support of operations.

Maintaining Situational Awareness on Adversary Forces in Peace Operations

Through a coordinated effort with several staff sections of the division staff, the Land Information Warfare Activity (LIWA) Forward Support Team (FST) Commander was able to focus and synchronize Information Operations built on information and force status on the FWFs' political, police, and military units. FM 100-6 provides an IO Mission Essential Task List (METL) which includes **"maintain a continuous estimate of potential adversaries and/or other operational situations in support of IO situational awareness and battlefield visualization."**[12]

Maintaining SA on the status and capabilities of the FWF military, para-military, police, and special police forces, and political entities in the MND-N sector of Bosnia and Herzegovina required the cooperation of several staff cells and the Brigades and Battalion Task Forces that make up the division. The LIWA FST Commander, as the head of the Division IO Cell, effected this coordination. In TFE, the key players in maintaining accurate information and force status on the FWFs were:

- **The Brigades and Battalion Task Forces;**
- **The Joint Military Commission;**
- **The UN-sponsored International Police Task Force;**
- **The division Political Advisor (POLAD);**
- **G-2;**
- **SOCCE Joint Commission Observers (JCOs).**

The Brigades and Battalion Task Forces developed an accurate status of the FWF military through scheduled Weapons Storage Site (WSS) inspections for compliance with authorized stockage levels. The results of these inspections and the authorized stockage levels were maintained by the G-2. The Joint Military Commission staff cell maintained a status on all approved convoys, mobilizations, and convoys conducted by the FWF forces and briefed the approved schedule at the Battle Update Brief (BUB) daily. The SOCCE's Joint Commission Observers (JCOs) were small teams of Special Forces soldiers who were passive collectors of intelligence while they carried out their primary mission of establishing effective liaison with civil leaders and agencies. The Division Provost Marshal (PMO) maintained liaison with the IPTF, with an IPTF officer often sitting in at the Division Main CP. The IPTF, in turn, monitored the conduct of FWF police and special police forces and informed the division through the PMO. The division commander's Political Advisor (POLAD) reported on the activities and status of political leaders and agencies through the political offices of the U.S. State Department, the Office of the High Representative, and other agencies operating in the AOR. The G-2 was the organizer of these reports and managed all intelligence data.

Through the Information Operations Working Group (IOWG), the LIWA FST Commander was able to act upon intelligence in support of information operations. He linked the various reports and intelligence summaries to accurately identify the Information Operations focus and direction.

IO Wargaming in Support of COA Analysis

During Operation JOINT GUARD, the Information Operations Working Group (IOWG) served as the Division's IO Cell for developing IO plans. Although the IOWG did not participate in division-level wargaming as a separate entity, all IOWG members were present at these wargaming sessions, and usually had already wargamed IO COAs in support of CONPLANs, and their branches and sequels during the regularly scheduled IOWG meetings.

Wargaming of IO campaign plans took place in the regularly scheduled meetings of the working group, and, at Division-level, G3-supervised wargaming sessions in the Division Main CP. Information Operations require detailed planning and longer lead time for execution to ensure all components of the IO Campaign are functioning during the "preparation of the objective phase" with non-lethal fires from the IO actors. These "non-lethal fires" should create the conditions for successful accomplishment of the operation and achieving the commander's desired end-state. For those events which could be anticipated, the IOWG conducted wargaming of the various IO COAs developed to arrive at a refined, coordinated, and synchronized IO Campaign Plan in support of the CONPLAN.

In Peace Operations, events, such as elections, resettlements, and weapons storage site inspections, are known well in advance. Other actors in the Global Information Environment, such as religious or political groups, may also plan their own events, which intrude into the Military Information Environment and affect military operations. Extremists may demonstrate, counter-demonstrate, boycott, or sabotage these events to derail the peace process. For events that were known in advance, the IOWG was able to develop a comprehensive IO Campaign that would support successful execution of military operations. Examples of such events include the municipal elections scheduled for September 1997, and the planned march of the Association of the Women of Sebrenica (WOS) to the Dulici Dam in Republika Serpska on 11 July 1997.

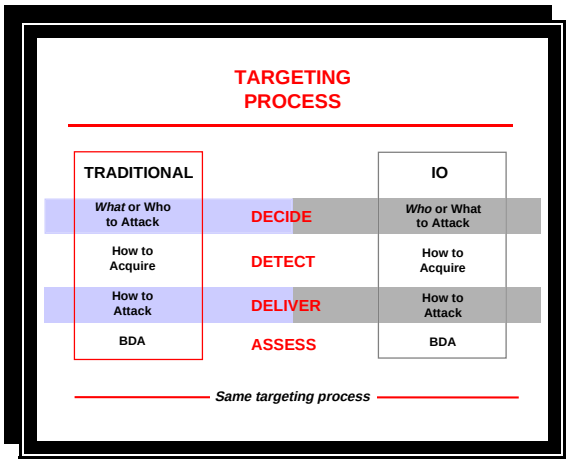
During a wargaming session held at the Division Main CP, and led by the G-3 around the map-table, the LIWA FST Commander responded to the G-2's "enemy actions" with the appropriate IO theme that had been developed to induce the desired behavior and the direct actions to be taken to support the desired endstate for the WOS march. The Division's IO actors (POLAD, PAO, JMC, PSYOP, CA, PMO, and Coalition Press Information Center) were present to discuss the specifics of how they would implement the IO themes into their operations and products. As the G-3 and G-2 talked through the *action-reaction-counter-action drills*[13], the conventional force actors were able to achieve an understanding of how the IO components contributed to the overall plan.

The IOWG conducted its own detailed wargaming for the municipal elections and the associated Division CONPLAN. The wargaming method used was a variation of the "avenue-in-depth technique."[14] The variation was that the focus was on the step-by-step process of the elections as opposed to a terrain avenue-of-approach focus. The working group developed themes for each phase of the elections process: registration of voters, electoral campaigning, balloting, tabulating ballots, international verification, and the implementation of the results in the form of a newly elected government. For each phase, the potential "enemy actions" were identified, as were the desired behaviors of the target audiences. The IOWG modified the action-reaction-counter-action drill to add the ***IO preventive action,*** essentially the theme in a product or message, that would induce the desired behavior in advance.[15] Through this wargaming process, the IOWG identified:

- **themes that supported the desired outcomes; and,**
- **the various IO products and actions the IO actors could develop and disseminate in support of the phased IO themes.**

The wargaming method of the action-reaction-counter-action drill was modified to include the preventive action of the IO theme that would elicit the desired behavior from the target audience prior to commencing operations. The IO Cell (in this case, the IOWG) was an active participant in division-level wargaming and conducted its own wargaming to develop IO themes, messages and products that supported the IO campaign component to division CONPLANs.

Integrating Targeting and Information Operations*



By using conventional targeting processes and redefining some IO terminology, TFE IO planners were able to incorporate lethal, nonlethal and information attack options into a uniquely synchronized plan for the commander. Targeting in peacekeeping and peace enforcement operations, while originally considered a different challenge from conventional coordination, has proven to be fundamentally the same as that used in high intensity operations. To use FM 25-100 terminology, the *tasks* which face the Division Targeting Team are no different in Bosnia, although the *conditions* and *standards* differ somewhat.

The major differences are the targeting objectives, which predominately shy away from physical destruction, and target sets, which overwhelmingly lean toward non-military entities. Instead of "hard" targets, such as multiple rocket launchers, air defense artillery sites and motorized rifle divisions, the high value targets (HVTs) and high payoff targets (HPTs) facing the peace enforcement commander are "soft" targets such as the intentions of government leaders, attitudes of the local populace, and influence over various social and political groups. In this environment, targeting takes a perspective which, up to now, has been considered by many to be the domain of information operations. However, during Operation JOINT GUARD, the unique capabilities of information operations (IO) were integrated into the targeting process to expand the maneuver commander's range of attack options.

Experience in Bosnia demonstrated that IO can be integrated into the conventional, tactical-level targeting process. In this manner, lethal, non-lethal and IO attack options are incorporated into the tactical decisionmaking process. Although this linkage is not readily apparent, both FM 6-20-10 (Targeting) and FM 100-6 (Information Operations) seek to provide the military commander lethal and non-lethal means to achieve the assigned mission. Conventional targeting describes both lethal (Fires and Maneuver) and non-lethal (EW and PSYOP) options, and IO describes attack options to strike at the adversary's personnel, equipment, communications, and facilities in an effort to disrupt or shape adversary C^2. Although lethal attack is always planned as a part of military operations, the main targeting effort during peace operations is non-lethal attack. In contrast to lethal attack, which normally targets hard military systems, IO uses non-lethal attack on people or C^2 nodes and targets attitudes, behavior, and intentions. Typical IO targets are civil, political, and military leaders who control or influence the local population, or assets that these leaders use to achieve their objectives.

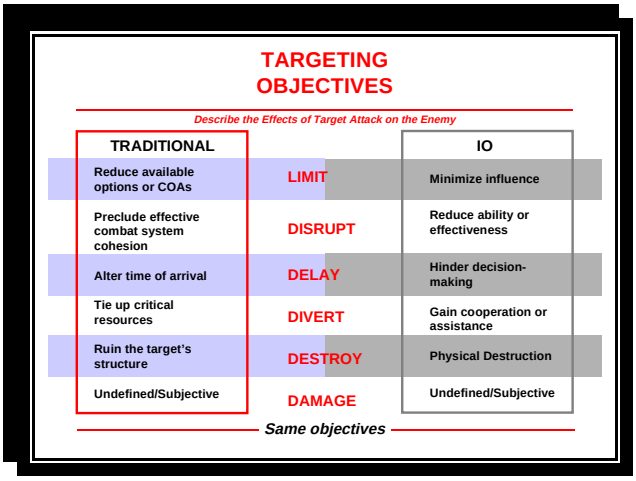
For example, if "adversary" leaders seek to turn a legal civilian political rally into a violent, hostile demonstration, the target set may be those capabilities and assets needed to form or transform a crowd (inflammatory radio broadcasts, loudspeaker vans, hand-held communication systems, crowd leaders). Additionally, if buses are necessary to transport people to the demonstration, the owner of the bus company could be targeted to discontinue his vehicular support for the demonstration and traffic control points may be set up on likely avenues of approach to delay or stop reinforcing buses. In some cases, there may be redundant processes working to attack an IO target, as is often done with conventional attack options against hard military targets. Critical C^2 nodes, such as telephone switchboards that transmit messages which instruct hostile crowds to assemble, can become a soft attack target by the use of electronic warfare assets. The creativity and innovation involved in such IO attack options are limitless, bounded only by the planners' ingenuity and the time available to plan.

*****This section was taken from an article submitted to the Center for Army Lessons Learned by CPT Robert Curris, Division Artillery, 1st Armored Division, and Mr. Marc Romanych, TFE LIWA, and later published as **"Integrating Targeting and Information Operations in Bosnia,"** in ***Field Artillery,*** HQDA PB6-98-4, July-August 1998, pp. 31-36.

Information Operations and Targeting

Integrating offensive IO into the targeting process starts by acknowledging the compatibility of conventional and IO targeting objectives. FM 6-20-10 describes targeting objectives which *Limit*, *Disrupt*, *Delay*, *Divert*, *Destroy*, and *Damage*. These terms are suitable to describe the objectives of IO, and TFE IO planners in Bosnia have provided some definitional clarity to these terms.

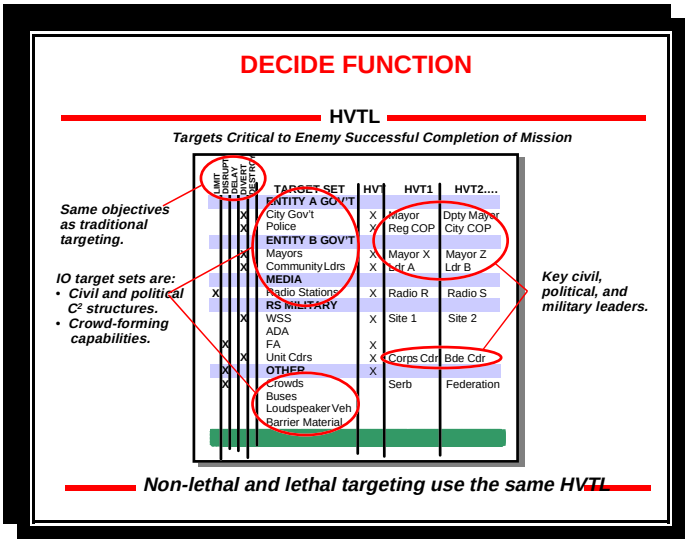
As both processes seek the same outcome, it holds that the process to achieve that outcome should be similar. Traditional targeting and information operations share the same endstate -- attacking enemy capabilities, and protecting friendly capabilities. To use parallel, non-intersecting planning processes is an inefficient and less than optimal use of limited planning time.



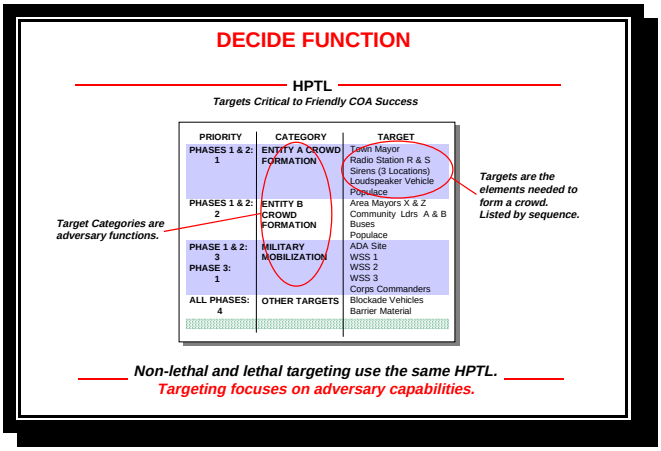
Decide

Once the tactical objectives are defined, conventional targeting can be used to identify the capabilities needed to achieve the stated conventional and IO objectives. The targeting methodology of *Decide*, *Detect*, *Deliver and Assess* (D^3A) provides the process to achieve the tactical commander's intent.

The *Decide* phase begins with clear commander's guidance, and ends by identifying the critical High Value and High Payoff Targets. One rule is to broaden some definitions, and include both hard and soft targets in the set of objectives. To this point, traditional targeting decisions have focused on the "what" (hard targets), while IO focuses on the "who" (soft targets). In military operations that include IO, the commander's intent will clearly include both sets. Expanding the definition to include both hard and soft targets allows for a truly integrated and comprehensive target set for the operation.



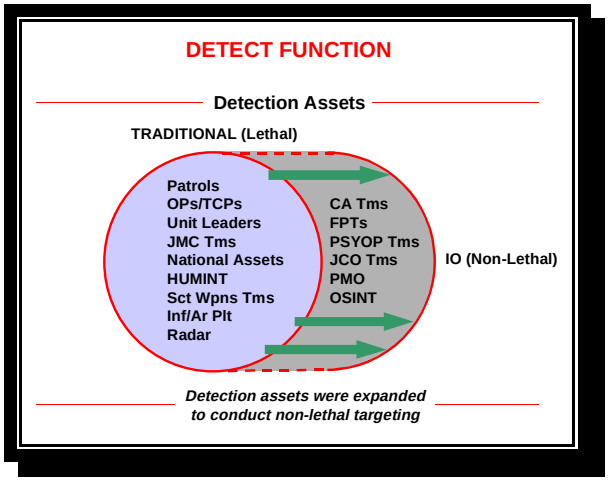
With this information, the G2 develops the High Value Target List (HVTL), which identifies the people or things (capabilities) critical to the enemy's success. The importance of a useful HVTL is that it portrays the stated tactical objectives (Limit, Delay, etc.) and includes hard and soft targets. Note that traditional targeting terms have been applied to non-traditional targets such as buses and government officials.



From the targets on the HVTL, the High Payoff Target List (HPTL) is developed to identify those targets (hard or soft) that are critical to the success of the friendly mission. The prioritization of the HPTL can differ between phases of an operation, but the list should remain the same and include all the required targets, from people to tanks etc. The development of the HVTL and the HPTL is the primary objective of the Decide function of targeting. The example formats used to display both of these products can be found in Annex C of FM 6-20-10 and work for both lethal and non-lethal targets without modification. Once the entire target list is compiled, the assignment of delivery means follows the traditional targeting process.

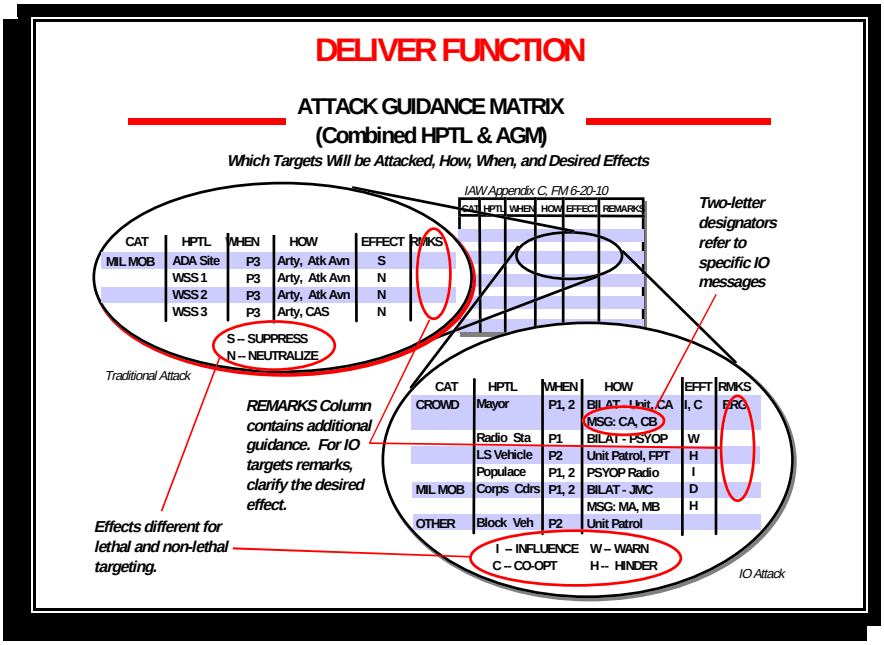
Detect

The *Detect* function begins with the collection plan. A critical point is that the collector/detectors for both hard and soft targets are predominately the same. Although additional HUMINT collectors are available in Bosnia, the IPB process and the Reconnaissance and Security Planning process do not need to be modified. This establishes the IO planner as a critical member of the intelligence team, and the targeting team.



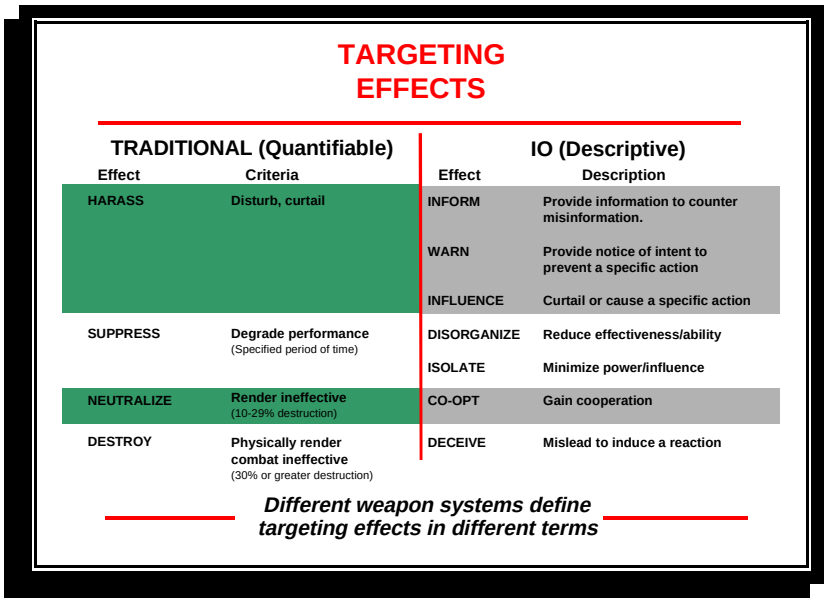
Deliver

Once the detection assets are aligned with the HVTs/HPTs, and appropriate NAIs and TAIs are established, *Delivery* assets are assigned against the targets. The prioritization and compilation of this data is effectively displayed on an Attack Guidance Matrix/High Priority Target List (AGM/HPTL), as illustrated in Annex C, FM 6-20-10. The AGM/ HPTL becomes the tool disseminated to the execution level. The AGM/HPTL provides the Who, What, When, How, and desired effect for each target. The matrix is simple to understand and has received positive feedback from units in the field for Operation JOINT GUARD. This matrix drives the Deliver phase of the process.



Assess

Assessment of the effects for both lethal and non-lethal attack is an on-going process throughout the operation, and requires dedicated assets to determine if objectives have been achieved, or require re-attack. The assessment phase follows the same process for both traditional and IO targeting. This requires a clear understanding of the desired endstate, as well as a capability to measure the effectiveness of the attack. In traditional targeting, desired effects are measured with the current doctrinal terms of *Harass, Suppress, Neutralize, and Destroy*. FM 100-6 does not include such definable terms for effects, but the IO personnel in Bosnia have developed the following IO effects matrix. The value of this matrix is the IO and Targeting Team's ability to develop new terminology for IO, but, at the same time, use somewhat the same lexicon as has been established by years of development by writers and users of Targeting doctrine.



BDA for C^2-Attack Information Operations

The METL in FM 100-6 for the IO Cell includes establishing C^2-Attack targeting and Battle Damage Assessment (BDA).[16] Information operations pose a unique challenge to the IO Cell in conducting BDA because the effects of C^2W on the enemy C^2 may not be in the form of physical damage. Instead, the effects may well be trends, activities, and patterns in future adversary actions.[17] BDA in IO is also known as "measures of effectiveness" or MOE. TFE was challenged to develop MOE which could assess the effectiveness of IO on "soft" target C^2-Attack.

C^2-Attack operations can be both "hard" and "soft" kill in effect.[18] "Hard kill" operations imply physical destruction with the application of lethal combat power, while "soft kill" operations achieve effects in attitudes and decisions. In peace operations, C^2-Attack operations will primarily be "soft kill" operations. The Information Operations Working Group, the IO Cell for Task Force Eagle, developed procedures to monitor the effectiveness of the radio component of the IO Campaign, a "soft kill" operation.

The MOE which TFE developed for "soft kill" IO C^2-Attack operations relied on subjective approach to assessing BDA, because IO planners needed to assess the emotions and attitudes of the target audiences. One MOE technique used was to interview the element which disseminated the IO message to get their impressions as to how the message was received, and whether the intended effect was achieved. Another MOE technique employed was to observe the actions of the intended target audience to verify that it responded to the IO message as intended. Interviewing random or selected members of the target audience for the reaction to the IO message is yet another method for measuring its effectiveness.[19] And lastly, monitoring the media of dissemination to ensure the message was transmitted is yet another method to measure whether the message reached the target audience. This last technique is explained in detail below, as it was applied to Radio PSYOP which used local radio stations to broadcast prepared IO messages in the local language.

During Operation JOINT GUARD, an "affiliate network" of 43 local radio stations within the MND-N Area of Operations disseminated information, in the form of SFOR and TFE press releases, and PSYOP messages.[20] The network covered most of the AO and included stations that were marketed toward each of the three FWFs. Many of the stations in the affiliate network provided this service at no cost to TFE and were receptive to reading the PSYOP-scripted messages, play the pre-recorded music tapes with Euro-pop, or use the press releases provided by the PSYOP Task Force (POTF). Some stations, mostly in the Republika Serpska, had to be induced into playing the tapes and scripts with payments of about 9 DM per minute.

The majority of radio stations in RS were state-controlled, while those in the Bosnian Federation were privately-owned. PSYOP products delivered over the radio waves consisted of PSYOP scripts to be read by the on-air announcer, pre-recorded music shows with PSYOP messages interspersed in the music segments, and Coalition Press Information Center (CPIC) and SFOR press releases. Live interviews with MND-N TF Commanders and live talk shows involving the local people discussing themes important to SFOR were two more means of using radio as a way to support the IO Campaign.

At the direction of the Commander Task Force Eagle (COMEAGLE), the IOWG developed a procedure to measure the level of compliance of the radio stations playing the scripted messages and pre-recorded programs. Live broadcasts of Commander interviews were verified on-site and required no monitoring program. The program developed sought to answer the following questions:

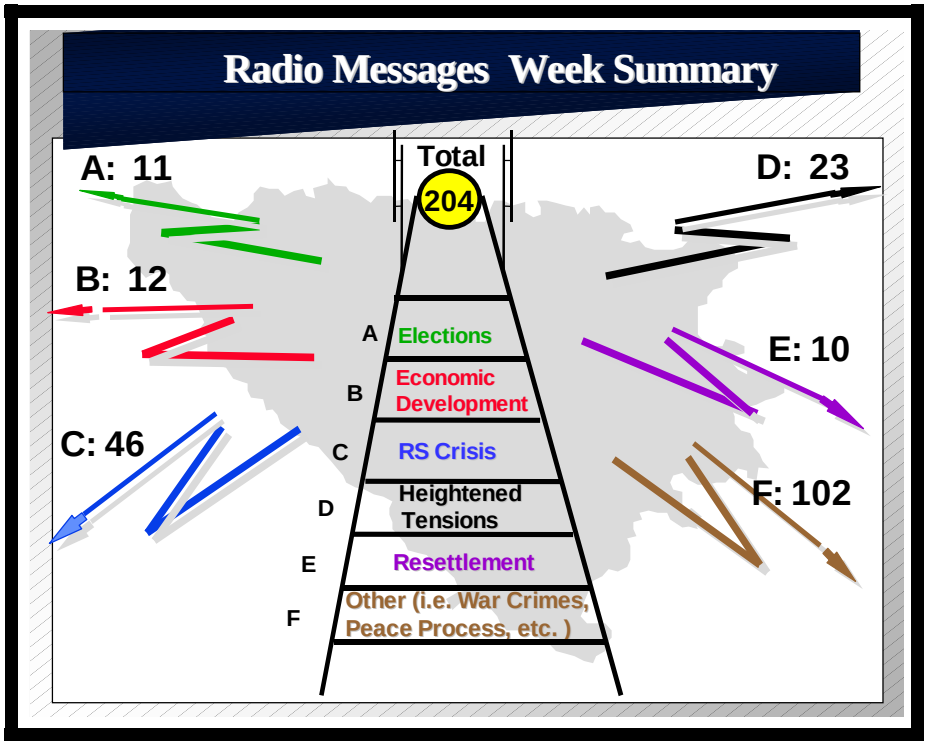
- **Are the radio stations playing the messages provided?**
- **What is the message clarity? Are the messages being modified in any way?**
- **Is the target audience receiving the message?**
- **What is the credibility of the station (i.e., does it have a reputation for honest reporting which gives equal treatment for all sides)?**

The IOWG was limited in its courses of action (COAs) for compliance-monitoring as it had limited assets with which to conduct the monitoring effort. The COA selected was to monitor three-five selected stations per week and conduct listener surveys. The stations were prioritized into three categories. First priority stations were those which TFE had to "pay for play," second priority stations were those marketing to key audiences, and third priority stations were all others.

The monitoring elements for TFE were the PSYOP Brigade PSYOP Support Elements (BPSEs) and Tactical PSYOP Teams (TPTs), the Joint Commision Observers (JCOs) under the direction of the Special Operations Command and Control Element (SOCCE), and the G-2 Open-Source Intelligence (OSINT) teams and Force Protection Teams (FPTs). The IO Cell produced the weekly FRAGO that assigned the monitoring elements the specified tasks. The PSYOP elements were tasked to conduct surveys of the target audiences of the radio stations being evaluated and, when possible, have supporting interpreters monitor the radio stations as part of the collection effort. The SOCCE was directed to have the JCO teams in the vicinity of the target radio station being evaluated monitor the station and document the accuracy of the messages and instances of false reporting or biased treatment of the issues. The G-2 OSINT and FPTs were directed to monitor specified stations in the same manner as the JCOs.

With these procedures, the IOWG was able to monitor and measure the effectiveness of the Radio component of the Information Campaign. Based on the results obtained, the DPSE could commend those stations which demonstrated compliance, and criticize those not in compliance, or, in the cases of "pay for play," withhold payment.

The technique employed by the TFE IOWG had the minimum impact on operations, using the same approach used to inspect weapons storage sites on a scheduled basis. Prioritizing the radio stations by category facilitated focusing the monitoring efforts on the high-payoff targets first. By providing feedback on radio operations, the DPSE could modify tactics, techniques and procedures where necessary to improve effectiveness. By monitoring radio station performance, the DPSE could ensure compliance for paid and free programming. The listener surveys provided feedback on whether or not the target audience was being reached. The figure below shows the number of PSYOP radio messages aired over a one-week period and the category of the messages.



Information Management in Support of Effective IO

"Given the advances in technology...it is easy to become awash in data. For this reason, a critical aspect of IO is getting the relevant information and intelligence (RII) that enables commanders to focus their efforts. Information operations are predicated on the right person receiving the right information in the right place and at the right time."[21]

Effective IO requires the fusion of information from a variety of sources. Technological advances in command, control, communications, computers, intelligence, surveillance, and reconnaissance systems (C^4ISR) confer an unprecedented ability to collect information from the battlespace. "The Army has transitioned from a time when the commander fought for information to a time when the commander is inundated with data even before he begins to fight for needed information. Information flow within the organization is complex yet vital to creating a clear picture for the commander. Optimum information flow within the organization requires both speed and clarity of transfer without creating an overabundance of fragmented or useless data. The organization designs an information management plan (IMP) to establish responsibilities and provide instructions on managing information."[22]

Information management has both procedural/organizational and technical aspects. From a procedural/organizational perspective, our ability to generate vast amounts of information from C^4ISR systems and reporting will make identification of the CCIR, PIR, routine unit status information, and the other kinds of information needed to make decisions more important to focus both collection and reporting.[23] Establishing effective procedures for managing and displaying reports and information inputs can reduce the phenomenon of "information overload" and improve C^2. Several BCTP Warfighter exercises have shown that C^2 problems experienced by division staffs are often attributed to information processing and management.[24]

From a technical perspective, "managing information includes managing the electromagnetic spectrum (EMS); deciding what sources and systems to use; ensuring a reliable flow of information between nodes and levels (horizontal and vertical integration); and resolving differences among information from multiple sources."[25] In peace operations where the force is multi-national in composition, information managers must establish a means and a plan to provide the RCP to all forces. Partners of the multi-national force with incompatible or less advanced C^4 systems may require interpreters, liaison officers (LOs), or augment these partners with equipment, operators and support to maintain the RCP effectively.[26]

Effective Information Management from both the procedural/organizational and technical aspects will enable the commander to fully leverage the capabilities of his INFOSYS to achieve information superiority and control the situation.

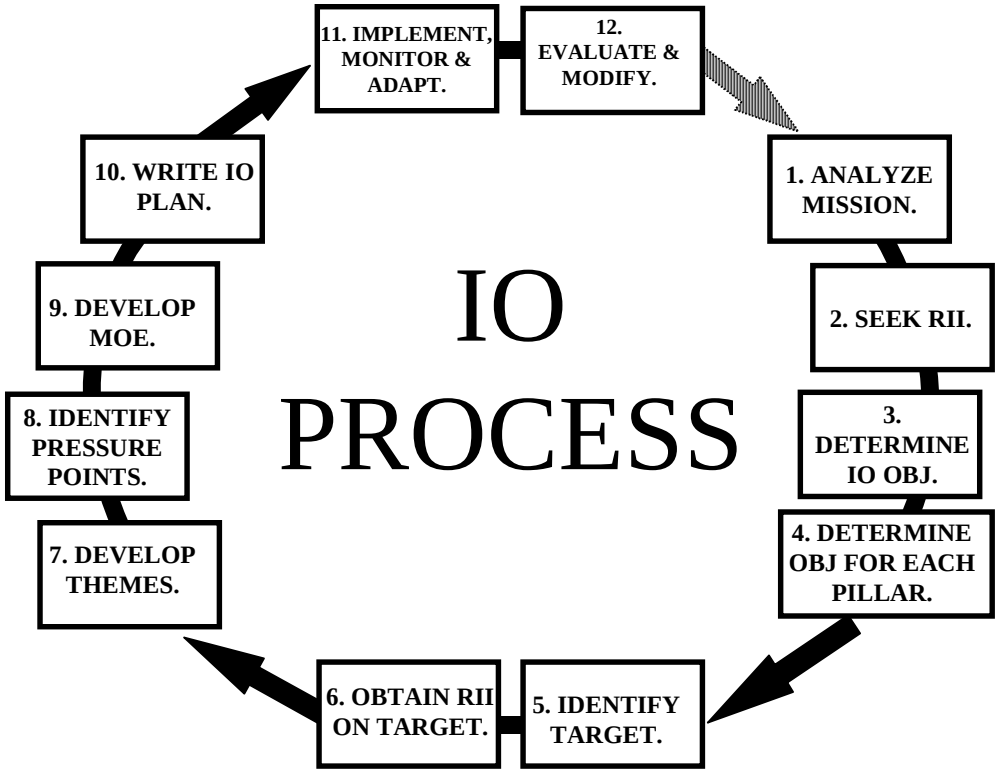
A Template of Operations Planning for the IO Staff

This template for planning, implementing, and evaluating IO focuses on the "perception management" piece of IO, also known as the "soft kill." C^2-Attack operations can be both "hard" and "soft" kill in effect.[27] "Hard kill" operations imply physical destruction with the application of lethal combat power, while "soft kill" operations achieve effects in attitudes and decisions. In peace operations, C^2-Attack operations will primarily be "soft kill" operations.

> **Perception Management:** ***Actions to convey or deny selected information and indicators to foreign audiences to influence their emotions, motives, and objective reasoning; and to intelligence systems and leaders at all levels to influence official estimates, ultimately resulting in foreign behaviors and official actions favorable to the originators objective.*** **(Joint Pub 1-02)**

IO Process

The IO process is a 12-step method that forms a template for planning, implementing, and evaluating IO. In applying this process, the reader should keep in mind that what Joint Pub 3-58 says of deception planning is true of the IO Process: **"Although diagrams of planning processes are useful in aiding the understanding of the individual elements of the process, it must be remembered that processes are seldom as linear as diagrams or flow charts may imply. Planners must be prepared to respond to the dynamics of the situation and of their own headquarters."** What follows are the 12 steps that the IO cell and the IOWG must follow to achieve effective Information Operations.



TECHNIQUES AND PROCEDURES

1. Analyze the Mission. The Division IO officer (this may be the LIWA FST Commander) and his cell analyze the mission to determine the military and political objectives and commander's intent. The IO cell collects all available Relevant Information and Intelligence (RII) and begins to formulate the questions that will need to be answered. If not already created, the G2 develops an IO Intelligence Preparation of the Battlefield. The Division IO Officer presents the work the IO cell completed to the Information Operations Working Group (IOWG). The other members of the IOWG analyze the mission to determine how they can best contribute to achieve the commander's objectives. In the IOWG, the LIWA FST Commander serves as a facilitator. His task is to exploit the creativity, talent, and experience of all the members. It is a team effort. And, although following the IOWG meetings the members will go back to their individual work sites to plan and manage their activities, it is through the IOWG that the Division IO Officer gains synergy by ensuring that IO is fully coordinated and synchronized. For the rest of the IO process, the reader can assume that the steps are carried out by the IOWG functioning as a team.

2. Seek RII. Relevant Information and Intelligence (RII) is the key to effective IO. It is needed to plan, implement, monitor, and evaluate. The G2 representative is the IO officer's link to RII. The IOWG develops Request for Intelligence (RFI), which the G2 representative works. He ensures RFIs are properly submitted, monitored, and answered, providing feedback to the IOWG. This does not mean the other members can sit back and wait for the "answers." They will be using their sources to collect RII. PSYOP, Civil Affairs (CA), CI, and SOCCE teams in the field will be collecting RII. The IO cell is aggressively exploiting the unclassified internet and the various military nets. The POLAD also has sources. The PAO will provide the IOWG with information on the media environment in which friendly forces are operating. Maintenance contact teams, logistics teams, engineers, reconnaissance elements, and Infantry and Military Police patrols are exploited for RII. The point is that the myriad of sources are fully exploited, and RII is shared within the IOWG.

3. Determine IO Objectives. An IO objective is a specific and operational statement regarding the desired accomplishments of the IO program. For each IO objective, the planner strives to use strong verbs, states only one purpose or aim, specifies a single end-product or result, and specifies the expected time for achievement.[28] It is important to remember that the closer the objectives are to outcomes that can be directly measured, the more likely it is that a competent evaluation will result. Using our scenario, the IO cell determines as an IO objective the following: "Within 90 days, dissuade the populace of town X from rioting." Dissuade is the strong verb. The IOWG has the one aim of dissuading the populace from rioting, and the specified outcome is the lack of rioting - the outcome that can be easily measured. The populace either riots or they do not. This IO objective becomes the overarching objective for each of the IOWG members. They will develop objectives for their individual elements of C^2W and Public Affairs (PA) and Civil Affairs (CA).

4. Determine Objectives for Each Element. The IO Staff Officer needs to know what the objectives of the elements of C^2W and PA and CA are and how they will aid in achieving the overarching IO objectives. Although members will come to the IOWG with objectives already in mind, it is important to go through a brainstorming process. Brainstorming takes up valuable time, but is time well spent. It fosters team ownership of the objectives; it provides a sanity check; and it allows the members to know each other's intent, creating opportunities for synergy. Brainstorming will ensure that the IO and the elements' objectives are clear, distinct, and focused, and, more importantly, will assist the members in understanding the connectivity between the elements' objectives and the overarching IO objective.

A PSYOP objective might be: Inform the target audience of the ramifications of any rioting. If ramifications include military response, it is imperative that the military and diplomatic agencies are capable and have the resolve to follow through on the military actions. This example illustrates why PSYOP themes must be approved by higher headquarters. (The approval process should not be that cumbersome. The objectives and themes for PSYOP, deception, and the other pillars of C^2W will be rolled into the IO program, which can easily be shown to support the CINC's IO campaign plan.) One might argue that "inform" is not a strong verb, and, admittedly, "inform" is a long way from "dissuade," but to simply inform is a necessary step toward achieving the IO objective, and is measurable. The military deception objective might be: Convince the target audience that certain areas will be heavily patrolled and monitored by ground and air assets. When in reality, the friendly assets are not available to conduct such operations as described. Electronic Warfare (EW) might have the objective to "Degrade and disrupt the capability of faction leaders to communicate electronically during a certain period of time." The time might be triggered by some event that indicates rioting is imminent. It must be remembered that the purpose of these objectives is to achieve the IO objective. Achieving an individual element's objective and not achieving the IO objective is a failure for the IOWG.

5. Identify IO Targets. The IO cell identifies IO targets and presents this list to the IOWG for additions and deletions; other IOWG members will have targets that the IO cell did not have. Targets will, of course, be quite diverse. They could be key communicators, a certain segment of the population, or a set of radio towers that are being used to encourage people to riot. The probability of success is increased if a target can be attacked by more than one pillar of C^2W.

6. Obtain Detailed Information about the Target Audience. As a minimum, RII about the target audience should consist of the following:

- ☛ **Political agendas.**
- ☛ **Biographic information.**
- ☛ **Decisionmaking processes.**
- ☛ **Demographic information: age, sex, race, religion, economic income, cultural likes and dislikes.**
- ☛ **The target's perceptions of friendly capabilities and possible courses of action.**
- ☛ **The target's IO capabilities and processes.**
- ☛ **Estimates of target's actions under differing scenarios.**
- ☛ **How the audience prefers to send, and especially to receive, their information, e.g., what percentages come from TV, Radio, and newspapers respectively?**

PSYOP personnel are trained in target audience analysis -- the process by which potential target audiences are identified and analyzed for effectiveness, accessibility, and susceptibility. This type of analysis prepares the IOWG for the next step -- developing themes.

7. Develop Friendly Information Themes. Army psychological operations doctrine defines a theme as a subject, topic, or line of persuasion used to achieve a psychological objective.[29] Themes to use and avoid will often be passed down from higher. However, that is not to say themes could not be developed at the Land Component level. The SFOR Information Campaign Themes during the fall of 1997 and Operation JOINT GUARD were:

- **The Establishment of a Secure Environment;**
- **Demining;**
- **Economic Recovery;**
- **The Rights of Displaced Persons, Refugees and Evacuees (DPREs);**
- **Acceptance of Election Results;**
- **The Proper Roles and Conduct of Civilian Police Forces;**
- **Arms Control; and**
- **Common Institutions supported by the Dayton Peace Accord.**[30]

PSYOP personnel have the skills, expertise, and experience to develop themes. But again, as with objectives, themes should be discussed within the IOWG for possible improvement and to ensure that all members are thoroughly familiar with them. Examples of possible themes include: "Peaceful protests is the appropriate way to communicate your desire for political change." "Violence will be met with force to protect lives and property." "Rioting will delay and possibly stop the rebuilding of roads and homes and the inflow of economic aid."

It is important to remember that IO themes are not necessarily PSYOP themes. Providing the right piece of information to the right audience with the purpose of reinforcing or creating perceptions or to cause ambiguity is the goal. However, thinking in terms of themes allows the IOWG to develop, identify and create that "right piece" of information.

8. Identify Pressure Points. A pressure point is an important, essential, or primary factor that can be influenced to control behavior. As with objectives and themes, the IO officer should facilitate an IOWG discussion with the purpose of identifying pressure points and ways that they can best be exploited. If the local population desperately needs economic aid, then such aid is a pressure point. In this case then, IO should communicate the message that the delivery of aid will depend on whether or not the political leaders support democracy.

9. Develop Measures of Effectiveness (MOE). Developing MOE for IO is, in my opinion, the most difficult step in the IO process. Without MOE, the IOWG will not be able to evaluate the effectiveness of the IO program. A commander has the right and the responsibility to ask his IO staff officer this simple question: "How do we know this IO stuff is helping me achieve my overall objectives?" Thus, the IOWG needs to build MOE into the IO plan so that the following three critical metrics can be measured:

★ ***Effectiveness.*** **Describes the relationship between outputs and objectives.** Were the IO objectives achieved? If not, why not?

★ ***Efficiency.*** **Describes the relationship of inputs and outputs.** Although the IO program may have been effective, could there have been ways to accomplish it quicker and cheaper?

★ ***Adaptability.*** **Describes the ability of the IOWG to respond to changing demands.** Was there sufficient flexibility to adjust a PSYOP program or deception plan to react to an unexpected event?

MOE can be classified as either quantitative or qualitative. "Quantitative methodology assumes the necessity, desirability, and even the possibility of applying some underlying empirical standard to social phenomena. By way of contrast, qualitative methodology assumes that some phenomena are not amenable to numerical mediation.[31]

10. Quantitative Research is Desirable When:

- ☛ **A picture of the environment at a given point in time is needed.**
- ☛ **Data that can be projected to a larger universe is needed.**
- ☛ **The target audience is difficult to reach.**
- ☛ **A large amount of specific information from the target audience is sought.**
- ☛ **The data must be statistically representative of a very large geographic *area.***

10. Qualitative Research is Desirable When:

- ☛ **Modifications need to be made in an idea before it is finalized.**
- ☛ **Very fast feedback from the targeted audience is needed.**
- ☛ **The research budget is limited.**
- ☛ **There is a need to probe deeply into the cause of some observed behavior.**[32]

The point here is that different kinds of assessments require different types of MOE. The IOWG should not get locked into thinking that if MOE are not quantifiable they are of no use.

11. Write the IO Plan. With the information obtained thus far, the IO cell is now ready to write the IO plan. The written document might be in the format of an IO Annex to a CONPLAN or OPLAN. In addition, the IO cell uses a series of worksheets, matrices, and giant charts to record and display objectives, pressure points, tasks, milestones, and timelines. Products used in TFE IO included:

- ● **Pressure Point Identification Worksheet (PPIW).** The PPIW provides the IO planner with a systematic way to identify ways to influence target audiences.
- ● **IO Planning Worksheet (PW).** The IO planner uses the PW to determine how and when to influence each pressure point.
- ● **Synchronization Matrix (SM).** The SM is used to deconflict and synchronize IO activity.
- ● **IO Implementation Worksheet (IW).** The IW is used to record additional information about each IO event found on the SM. In addition to identifying the attack "subsystem," the worksheet identifies the specific information themes that will be used for each IO audience.
- ● **IO Implementation Matrix (IM).** The IM chronologically lists all IO executions for each IO function. Information from the IM is carried forward to the optional IO Implementation Graphic.

12. Implement and Monitor the IO Campaign Plan. During this step, the plan is executed. The plan is monitored and feedback begins to be collected. The collection of RII continues. A Synchronization Matrix is used to deconflict and synchronize IO activity. The members of the IOWG are constantly using RII, MOE, and feedback to evaluate the effectiveness of their individual activities, allowing them to fine-tune the plan and adjust to unexpected events. The focus is on coordinating, adapting, and achieving synergy.

Endnotes, Chapter Six

[1] Headquarters, Dept. of the Army, **Field Manual 100-6,** ***Information Operations,*** (Washington, DC: USGPO, 27 August 1996), p. D-0.
[2] David L. Grange, Maj. Gen., U.S. Army, and James A. Kelley, Col., U.S. Army, **"Information Dominance,"** ***Army,*** March 1997, p. 37.
[3] Craig Jones, Lt. Col. (Ret.), U.S. Army, **"The IO Process,"** ***News from the Front!,*** Center for Army Lessons Learned, March-April 1998, pp. 1-8.
[4] Center for Army Lessons Learned, ***B/H CAAT V Initial Impressions Report – Task Force Eagle Transition,*** (Unclassified, Distribution Limited, Fort Leavenworth, KS: CALL), May 1997, p. 22.
[5] Ibid., p. 6-7.
[6] Ibid.
[7] Jeffrey P. Jones and Michael P. Mathews, **"PSYOP and the Warfighting CINC,"** ***Joint Forces Quarterly,"*** Summer 1995, No. 8, p. 32.
[8] Land Information Warfare Activity (LIWA), ***Introduction to Information Campaign Planning and Execution,*** Student Materials prepared for the LIWA by SYTEX Inc., Vienna, VA, May 1998.
[9] Center for Army Lessons Learned, ***B/H CAAT XIII, Initial Impressions Report (DRAFT),*** (Unclassified, Distribution Limited, Fort Leavenworth, KS: In Press), June 1998, CALLCOMS observation 10000-85008.
[10] See Observation: "Task Force Eagle's DTOC is not organized like a normal heavy division's TOC," Center for Army Lessons Learned, ***BH CAAT 2 Initial Impressions Report,*** (Unclassified, Distribution Limited, Fort Leavenworth, KS: CALL), September 1996, p. C-67.
[11] See Center for Army Lessons Learned, ***B/H CAAT 3-4 Initial Impressions Report,*** (Unclassified, Distribution Limited, Fort Leavenworth, KS: CALL), March 1997, p. 5.
[12] Headquarters, Dept. of the Army, ***Information Operations,*** **Field Manual 100-6,** 27 August 1996, p. D-2.
[13] U.S. Army Command and General Staff College, Student Text 101-5, ***Command and Staff Decision Processes,*** Fort Leavenworth, KS: CGSC Press, 20 February 1996, p. 4-20.
[14] Ibid., p. 4-7.
[15] Ibid., pp. 4-20 to 4-21.
[16] Headquarters, Dept. of the Army, ***Information Operations,*** **Field Manual 100-6,** op. cit., p. D-3.
[17] Headquarters, Dept. of the Army, ***Intelligence and Electronic Warfare Operations,*** **Field Manual 34-1,** op. cit., p. 7-2. See also, Headquarters, Dept. of the Army, ***Information Operations,*** **Field Manual 100-6,** op. cit., p. 4-7.
[18] Headquarters, Dept. of the Army, ***Information Operations,*** **Field Manual,** op. cit., p. 2-4.
[19] Center for Army Lessons Learned, ***B/H CAAT XIII, Initial Impressions Report (DRAFT),*** (Unclassified, Distribution Limited, Fort Leavenworth, KS: CALL), In Press, June 1998, CALLCOMS observation 10000-29594.
[20] The collection of radio stations was not a network in the sense that they were under one controlling authority; rather, they represented that portion of available radio stations which cooperated with the DPSE-managed PSYOP radio message program. The "network" included stations representing all three of the FWFs, and expanded as the DPSE was able to induce radio station owners or managers to cooperate.
[21] David L. Grange, Maj. Gen., U.S. Army, and James A. Kelley, Col., U.S. Army, **"Information Dominance,"** ***Army,*** March 1997, p. 34.
[22] Combined Arms Doctrine Directorate (formerly Corps and Division Doctrine Directorate), U.S. Army Command and General Staff College, ***Operations,*** **Field Manual 100-5, Final Draft,** 5 August 1997, Chapter 19, **"Information Operations,"** p. 19-3.
[23] James M. Dubik, Col., U.S. Army, ***Creating Combat Power for the 21st Century,*** **The Land Warfare Papers,** Arlington, VA.: Association of the United States Army, Institute of Land Warfare, No. 25, October 1996, p. 6.

[24] Thomas D. Morgan, Lt. Col. (Ret.), U.S. Army, **"BCTP: Training Leaders,"** ***Military Review,*** July 1990, Vol. LXX, No. 7, pp. 42-52.
[25] Headquarters, Dept. of the Army, ***Information Operations,*** **Field Manual 100-6,** op. cit., p. 2-13.
[26] Headquarters, Dept. of the Army, ***The Army in Multinational Operations,*** **Field Manual 100-8,** op. cit., p. A-4.
[27] Headquarters, Dept. of the Army, ***Information Operations,*** **Field Manual 100-6,** op. cit., p. 2-4.
[28] Peter H. Rossi and Howard E. Freeman, ***Evaluation,*** Beverly Hills, CA: SAGE Publications, 1982, p. 59.
[29] Headquarters, Dept. of the Army, ***Psychological Operations,*** **Field Manual 33-1,** (Unclassified, Distribution Limited), op. cit., p. Glossary 12.
[30] Center for Army Lessons Learned, ***B/H CAAT XI, Initial Impressions Report,*** (Unclassified, Distribution Limited, Fort Leavenworth, KS: CALL), April 1998, p. A-18, CALLCOMS observation 10000-13978.
[31] Michael Quinn Patton, ***Utilization-Focused Evaluation,*** Beverly Hills, CA: SAGE Publications, 1978, p. 212.
[32] Thomas L. Greenbaum, ***The Handbook for Focus Group Research,*** New York, NY: Lexington Books, 1993, p. 30.